VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA SYSTÉMOVÉHO INŽENÝRSTVÍ

Návrh počítačové sítě pro obchodní firmu

Design of Computer Network for Bussiness Company

Student: Jakub Kyselý

Vedoucí bakalářské práce: Ing. Petr Rozehnal, Ph.D.

Ostrava 2017

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání bakalářské práce

Student: **Jakub Kyselý**

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: 6209R017 Informatika v ekonomice

Téma: Návrh počítačové sítě pro obchodní firmu
Design of Computer Network for a Bussiness Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Úvod
2. Popis technologii a základních pojmů počítačových sítí
3. Analýza současného stavu počítačové sítě a prostředí
4. Návrh řešení počítačové sítě
5. Zhodnocení řešení počítačové sítě
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.
KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Rozehnal, Ph.D.**

Datum zadání: 18.11.2016
Datum odevzdání: 05.05.2017

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Zdeněk Zmeškal
děkan fakulty

Chtěl bych vyjádřit poděkování vedoucímu bakalářské práce Ing. Petru Rozehnalovi, Ph.D. za odborné vedení a cenné rady při zpracování této bakalářské práce a také vedení firmy EXTRAVÝFUK, s. r. o. za umožnění spolupráce. Poděkování za morální podporu a trpělivost patří mé rodině, přátelům a zejména mé přítelkyni.

Prohlašuji, že jsem celou práci, včetně všech příloh, vypracoval samostatně.

V Ostravě dne 4. 5. 2017

.....

Jakub Kyselý

Obsah

1 Úvod

Od dob, kdy byla vyvinuta první počítačová síť, se mnohé změnilo. Od malých, jednoduchých a pomalých sítí, které byly využívány většinou vědeckými, výzkumnými a vojenskými pracovišti, jsme se dostali k celosvětově rozšířeným počítačovým sítím, které se staly doslova součástí našeho každodenního života jak v práci, ve škole, tak dokonce i doma. Tyto počítačové sítě jsou komplikovanější, rozsáhlejší a rychlejší, než jsme si v minulosti dokázali představit.

V této bakalářské práci bude cílem návrh počítačové sítě s využitím moderních technologií s výhledem vyspělosti sítě pro budoucí potřeby firmy a poté zhodnocení navrhnuté počítačové sítě, a to pro pobočku obchodní firmy EXTRAVÝFUK, s. r. o., která se nachází ve Frýdku-Místku. Konkrétně bude cílem této práce návrh fyzické i logické struktury počítačové sítě včetně aktivních i pasivních hardwarových prvků sítě, které zlepší odezvu, rychlost, dostupnost, a hlavně spolehlivost počítačové sítě jak v rámci interní sítě firmy, tak také do venkovní sítě internet. Dále budou navrhnuty podle požadavků firmy koncové zařízení, jako jsou síťové tiskárny, které umožní bezproblémový tisk takřka odkudkoliv, IP kamery kvůli dohledu nad zaměstnanci a také z důvodu bezpečnosti majetku firmy, a nakonec síťové úložiště, které umožní ukládání a zálohování veškerých citlivých dat ve firmě.

Tyto změny se rozhodla firma udělat z důvodu nespolehlivosti současné sítě, potřeby rozšířit tuto síť a nakonec vyřešit ukládání bezpečnostních záznamů ze zabezpečovacích IP kamer včetně streamování do vnější sítě internet, rozšíření koncových zařízení a také zálohování všech citlivých firemních dat na síťové úložiště ve firmě.

Ve druhé kapitole budou popsány technologie a základní pojmy počítačových sítí, které byly využívány v této bakalářské práci.

Třetí kapitola bude zaměřena na analýzu současného stavu počítačové sítě a prostředí, ve kterém obchodní firma EXTRAVÝFUK, s. r. o. funguje a v kterém bude počítačová síť realizována. Budou zde popsány základní charakteristiky společnosti, analýza prostředí a počítačové sítě, a nakonec požadavky firmy na návrh nové počítačové sítě.

Kapitola čtvrtá je zaměřena na problematiku návrhu počítačové sítě. Bude zde navrhnuta změna připojení firmy k internetu, samotný návrh počítačové sítě, který bude obsahovat návrh využitých aktivních i pasivních hardwarových prvků sítě, a následné jejich fyzické a logické propojení, a nakonec jejich nastavení. Bude zde také návrh

a nastavení nových koncových zařízení tak, aby bylo umožněno bezproblémové fungování těchto koncových zařízení podle požadavků firmy.

Dále bude zhodnoceno řešení počítačové sítě, a to v předposlední páté kapitole. Konkrétně zde bude zhodnocení návrhu sítě z funkčního a finanční hlediska, které je jedno z hlavních bodů realizovatelnosti.

2 Popis technologií a základních pojmů počítačových sítí

2.1. Dělení počítačových sítí podle rozlehlosti

Sítě se dají rozdělit podle několika kritérií, ovšem mezi hlavní patří právě rozdělení podle rozlehlosti, kterým se tato část kapitoly zabývá.

2.1.1. PAN

Kupříkladu síť PAN (Personal Area Networks), která je nejmenší ze všech sítí, nazývá se také osobní síť. Je uskutečněna hlavně technologií bluetooth (Sosinsky, 2010).

2.1.2. CAN

Méně častá je univerzitní síť CAN (Campus Area Network), která pokrývá skupinu budov a to např. fakulty, knihovny nebo koleje (Sosinsky, 2010).

2.1.3. MAN

Dále také existuje síť MAN (Metropolitan Area Network) také zvaná metropolitní, či městská síť, která je menší než síť WAN, ale větší než síť LAN, které jsou více popsány níže (Sosinsky, 2010; Horák, Keršláger, 2011).

2.1.4. LAN

Avšak nejdůležitějšími a nejpřínosnějšími sítěmi pro tuto práci jsou sítě WAN a LAN. LAN (Local Area Network) je lokální síť působící na malém území, je privátní a má omezený počet domén či podsítí. Konkrétněji je to skupina propojených systémů působící v jedné místnosti, jednom patře, jedné budově nebo mezi malým počtem počítačů propojených rozbočovačem (Sosinsky, 2010; Horák, Keršláger, 2011).

2.1.5. WAN

Nejrozsáhlejší ze všech sítí je síť WAN (Wide Area Network). Jedná se o globální síť čili spojení více sítí MAN a LAN, tyto sítě mohou být spojeny metalickými i optickými kabely a stejně tak i bezdrátově. Jelikož geografický dosah sítě roste kvůli připojování uživatelů v různých městech a státech, sítě MAN a LAN přerůstají právě ve WAN. Sítě WAN se rozprostírají po ploše několika desítek kilometrů a mohou mít dosah mezi celými státy nebo dokonce kontinenty. Počet uživatelů se pohybuje v desítkách tisících. Mnoho

sítí WAN bývá vybudována soukromě, většinou poskytovateli telekomunikačních služeb. Příkladem této sítě je celosvětová síť Internet (Horák, Keršláger, 2011).

2.2.Topologie počítačových sítí

Obsahem této části kapitoly je topologie počítačových sítí. Způsob, jakým jsou počítače v síti propojeny, se nazývá právě topologie, která je prvkem síťového standardu. Topologie také podstatně určuje výsledné vlastnosti sítě a úzce souvisí s kabeláží.

2.2.1. Sběrnicová topologie (Bus)

Počítače jsou zapojeny průběžným vedením, a to od počítače k počítači. K vedení se připojují odbočovacími prvky (např. T konektorem). Sběrnicová topologie je většinou využívána v sítích s koaxiálním kabelem. Tato topologie má své výhody a nevýhody. Výhodou je malá spotřeba kabelu a také jeho nízká cena. To kvůli řetězovému zapojení počítačů. Naopak jednou z nevýhod je velký počet spojů v kabelu, tento problém způsobuje mnoho potíží a zvyšuje poruchovost. Další nevýhodou je možné přerušení komunikace mezi všemi počítači. Ta je závislá na celém principu této topologie, pokud dojde k jakémukoliv přerušení, havaruje celá síť (Horák, Keršláger, 2011).

2.2.2. Kruhová topologie (Ring)

Jak vyplývá z názvu, základem této topologie je souvislý kruh. Kruh je vytvářen spojovacím vedením mezi počítači, díky čemu je možné používat metodu postupného předávání zpráv zvané token. Tudíž výhodou této topologie je pravidelné předávání zpráv v kruhu. Jeho nevýhodou je, podobně jako u sběrnicové topologie, přerušení vodiče. Proto se stejně jako u sběrnice může porouchat celá síť. Tento problém se řeší zdvojováním kabelu (např. u sítí IBM Token Ring) (Horák, Keršláger, 2011).

2.2.3. Hvězdicová topologie (Star)

U této topologie záleží nejvíce na rozbočovači, který tvoří střed sítě. Rozbočovačem může být koncentrátor či hub, které se používaly převážně kdysi, v dnešní době se ve většině případů využívá switch. K rozbočovači jsou soustředěny kabely počítačů. Každý počítač je připojen vlastním kabelem, a to nejčastěji kroucenou dvojlinkou. Hvězdicová topologie je dnes nejpoužívanější topologií ze všech. Výhodou této topologie je malá pravděpodobnost vzniku chyby. Pokud vznikne porucha jednoho kabelu, za následek bude pouze vyřazení z činnosti jedné sítě. V porovnání se sběrnicovou

topologií je u hvězdicové topologie jednodušší lokalizovat poruchu. Z toho vyplývá, že hvězda je spolehlivá a rychlá. Nevýhodou je bohužel nutnost koncentrátoru (Horák, Keršláger, 2011).

2.2.4. Stromová typologie (Tree)

Tato topologie je založena na rozvětvování. Je odvozena od kořenové úrovně, která je zároveň tou nejvyšší. V této úrovni se nachází pouze jeden uzel, který je propojen s uzly druhé úrovně, která se nachází pod ní. Dále se tyto uzly v druhé úrovni propojují s dalšími, a to s jedním anebo více uzly třetí úrovně. Takto se dá pokračovat dál a větvit na další úrovně. Nicméně pro základní stromovou topologii musí existovat nejméně tři úrovně. V opačném případě by došlo ke tvaru topologie hvězdy. Pokud selže jeden uzel druhé úrovně, ostatní části sítě mohou nadále fungovat, také je nízká spotřeba kabelů, což jsou výhody stromu. Na druhou stranu nevýhodou je opět nutnost koncentrátoru, stejně jako u hvězdicové topologie, jelikož strom se skládá ze spojení hvězd (Sosinsky, 2010).

2.3. Architektura TCP/IP

Zkratka tohoto modelu vznikla spojením názvů dvou protokolů: TCP (Transmition Control Protocol – protokol řízení přenosů) a IP (Internet Protocol). TCP/IP je vlastně sada protokolů a standardů, nejen těch již zmiňovaných, ale také dalších, které zasílají data na sítích s přepínáním paketů (Sosinsky, 2010).

2.3.1. Protokol TCP

Protokol TCP slouží k zavádění virtuálních spojení mezi dvojicemi koncových bodů. Také má na starost řízení přenosu dat a jejich doručení. Technologie TCP obsahuje informace, které se označují jako data TCP. To, jak tento protokol funguje, má vliv na výkonnost, ale hlavně na naprostou většinu internetové komunikace a architektury aplikací (Sosinsky, 2010).

2.3.2. Protokol IP

Protokol IP je využit k zabalení dat zasílaných do sítě s přepínáním paketů, zabývá se také adresací systémů v síti. Jednotlivé pakety se zasílají právě prostřednictvím protokolu IP (Sosinsky, 2010).

IP adresa (Internet Protocol)

IP adresa slouží k identifikaci síťového rozhraní v počítačové síti, která používá IP protokol, který umožňuje komunikaci všech zařízení v Internetu. IP adresa je v určitém tvaru čísel daném verzí protokolu. Existuje IPv4 adresa neboli IP verze 4 a IPv6 adresa. Liší se v adresním prostoru a zápisu, IPv4 adresa je 32bitová a je zapisována čtyřmi desítkovými čísly, která jsou oddělena tečkami. Nicméně IPv4 adresy byly vyčerpány a nastupují již zmíněné IPv6 adresy. Ty využívají 128bitové IP adresy, ta je zapsána v hexadecimálním tvaru jako osm skupin po čtyřech číslicích tentokrát oddělených dvojtečkami (Odom, 2005).

Třída A

U této adresy je celkových 32 bitů rozdělených na 8 a 24 bitů. Síťová část IP adresy je zastoupena 8 bity, k identifikaci koncových stanic a zařízení je určených zbývajících 24 bitů. IP adresy třídy A jsou tudíž vybaveny IP adresami pro ohromné množství koncových zařízení (přibližně 16 milionů IP adres, 2^{24}). IP adresy třídy A jsou typické binárním zápisem začínajícím nulou (Odom, 2005).

Třída B

Bity jsou rozděleny přesně na polovinu, takže 16 bitů zastupuje síťovou část IP adresy a 16 bitů slouží k identifikaci koncových zařízení. Síť třídy B má tedy nižší rozpětí (asi 65 tisíc IP adres, neboli 2^{16}) než třída A, a používá se pro střední až velké množství počítačů. V binárním zápisu začíná jedničkou a nulou (Odom, 2005).

Třída C

V tomto případě je rozvržení bitů opačné oproti třídě A, z toho vyplývá 24 bitů pro zastoupení síťové části IP adresy a zbylých 8 bitů pro identifikaci koncových zařízení. Síť třídy C je vhodná pro malé sítě (254 IP adres, 2^8). V binárním zápisu začíná dvěma jedničkami a nulou (Odom, 2005).

Třída D

Třída D je určena pro vysílání pro předem určenou skupinu zařízení (multicast). Binární zápis této třídy začíná třemi jedničkami a nulou (Odom, 2005).

Třída E

Tyto třídy se využívají pouze pro výzkumné účely, nikoli pro adresování běžných zařízení. Binárním zápisem třídy E je adresa začínající čtyřmi jedničkami (Odom, 2005).

Maska podsítě

Pomocí masky podsítě můžeme zjistit, která část identifikuje síť a která koncové zařízení. Je to také 32bitové číslo, zleva začínající jedničkami a pokračující nulami. Adresy sítě jsou vyjádřeny jedničkami v masce, bity v IP adrese, které jsou součástí adresy koncového zařízení, tak jsou určeny nulami (Odom, 2005).

2.3.3. Model TCP/IP

Tento síťový model je spolu s ISO/OSI nejznámějším modelem. Model TCP/IP se využíval ve vývoji internetu více než ISO/OSI, který je spíše teoretickou pomůckou k porozumění síťové komunikaci (Spurná, 2010).

Model má čtyři vrstvy: 1. Vrstva síťového rozhraní
2. Internetová vrstva
3. Transportní vrstva
4. Aplikační vrstva

Vrstva síťového rozhraní

Vrstva síťového rozhraní je dobrá k tomu, aby měla data přístup na síť, také ke kontrole zařízení a síťových médií na síti (Spurná, 2010).

Internetová vrstva

Internetová vrstva zajišťuje to, aby se data dostala k cíli tou nejlepší možnou cestou (Spurná, 2010).

Transportní vrstva

Transportní vrstva zajišťuje vzájemnou komunikaci vzdálených zařízení napříč sítí a spolehlivý přenos dat (Spurná, 2010).

Aplikační vrstva

Aplikační vrstva slouží k tomu, aby se uživateli zobrazila koncová data spolu s kódováním (Spurná, 2010).

2.4.Model ISO/OSI

Tento model obsahuje sedm následujících vrstev: 1. Fyzická vrstva
2. Spojová vrstva
3. Síťová vrstva
4. Transportní vrstva
5. Relační vrstva
6. Prezentační vrstva
7. Aplikační vrstva

2.4.1. Fyzická vrstva

Fyzická vrstva musí zajistit vysílání dat na fyzické médium. Přebere datový rámec z vrstvy nad fyzickou – spojové vrstvy, poté překóduje binární vyjádření rámce do signálu a ten odvysílá na médium. A naopak z druhé strany získá signál z přenosového média, který převede na jedničky a nuly (digitální kód), poté jej předá spojovací vrstvě ke zpracování (Spurná, 2010).

2.4.2. Spojová vrstva

Spojová vrstva má za úkol přípravu paketů ze síťové vrstvy pro přenos na přenosové médium a zároveň zkontrolovat přístup na toto přenosové médium. Data z vyšších vrstev přejdou do spojové vrstvy, kde jsou připraveny vytvořením datových rámců pro vyslání na přenosové médium, tato vrstva také přijímá data ze sítě. Na této vrstvě pracují přepínače, mosty a síťové karty (Spurná, 2010).

2.4.3. Síťová vrstva

Síťová vrstva zajišťuje, že se jednotlivé části zprávy dostanou do cílového zařízení. Cílové zařízení může být i ve vzdálené síti. Také zaručuje adresování a zapouzdření dat do paketu (datová jednotka vzniklá v síťové vrstvě). Data vrstva přijala z vyšší – transportní vrstvy. Po tomto procesu má vrstva ještě za úkol směrování a rozbalení paketu. Na této vrstvě pracují směrovače.

Protokoly této vrstvy: IP, ICMP, ARP (Spurná, 2010).

2.4.4. Transportní vrstva

Transportní vrstva propojuje síťovou vrstvu a relační vrstvu. Zajišťuje více současných přenosů, a to díky údajům o zdrojovém a cílovém portu obsažených v této vrstvě. Tyto

porty slouží k rozpoznání procesu (aplikace), který má zpracovat daná data. Transportní vrstva musí zpracovat tato data do správné velikosti a formátu pro síťovou vrstvu.

Protokoly této vrstvy: TCP, UDP (Spurná, 2010; Sosinsky, 2010).

2.4.5. Relační vrstva

Relační vrstva zajišťuje a synchronizuje přenos mezi relačními vrstvami obou stran. Relaci také vytváří, obnovuje nebo ukončuje mezi protistranami. Základními prvky této vrstvy jsou bezpečnostní mechanismy, příkladem tohoto mechanismu je přihlašování k relaci nebo další podoby dialogu s uživatelem.

Protokoly této vrstvy: NetBIOS, Apple Talk, SSL (Spurná, 2010; Sosinsky, 2010).

2.4.6. Prezentační vrstva

Prezentační vrstva převádí data do tvaru (formátuje), ve kterém je pro aplikaci čitelný. Prezentační vrstva přijímá data z aplikační vrstvy, data formátuje, probíhá zde také volitelná komprese a šifruje je. Poté data předá relační vrstvě. Pokud se v této vrstvě objeví data z relační vrstvy, pak je dekomprimuje a dešifruje. To proto, aby data z relační vrstvy byla převedena do tvaru, které rozumí aplikační vrstva. Používá protokoly pro smazání rozdílů mezi operačními systémy a aplikacemi. Tak počítač, který má například znakovou sadu ASCII, může komunikovat s počítačem, který používá jinou znakovou sadu založenou na ASCII, anebo zcela jinou znakovou sadu, jako je třeba Unicode (Spurná, 2010; Sosinsky, 2010).

2.4.7. Aplikační vrstva

Aplikační vrstva slouží ke spolupráci aplikací na obou stranách přenosu, zajišťuje spojení mezi aplikací a sítí. Aplikační vrstva je velmi rozmanitá a poskytuje mnoho služeb, nejčastějšími funkcemi, které poskytuje, jsou například vlastnosti zobrazení, e-mail, přenosy souborů, síťový tisk, provádění a správa vstupně výstupních operací, nebo vyhledávání informací v adresářových službách. Programy této vrstvy jsou webové prohlížeče, e-mailoví klienti, řádková rozhraní, příkazové řádky, kancelářské balíky a další.

Protokoly této vrstvy jsou HTTP, FTP, TFTP, DNS, DHCP, SMTP, POP3, IMAP, SSH, … (Spurná, 2010; Sosinsky, 2010).

2.5.Srovnání protokolů

Popisované protokoly lze srovnat, protokoly TCP/IP je možné popsat více podrobně i v ISO/OSI modelu. Aplikační vrstva TCP/IP modelu je v ISO/OSI modelu detailněji rozložena do tří vrstev, a to do aplikační, prezentační a relační vrstvy. Transportní vrstvy se nacházejí v obou modelech a zabývají se rozdělením jednotlivých současně probíhajících datových přenosů mezi zdrojovým a cílovým zařízením, také popisují, jak si počítače navzájem potvrzují předaná data, jak se chovají při chybném přenosu dat a jak je rozdělují do segmentů, které jsou počítači následně posílány a rekonstruovány v původním pořadí. Dalšími vrstvami jsou síťová a internetová, ty se zabývají, jakým způsobem jsou data směrována po síti směrem k cílovému zařízení a obě také popisují IP protokol, který se směrováním zabývá. V modelu TCP/IP se nachází vrstva síťového rozhraní, ta je v modelu ISO/OSI rozdělena do dvou vrstev – spojové a fyzické vrstvy. Porovnání těchto dvou modelů lze vidět v Tabulce 2.1.

ISO/OSI model	TCP/IP model
Aplikační vrstva	Aplikační vrstva
Prezentační vrstva	
Relační vrstva	
Transportní vrstva	Transportní vrstva
Síťová vrstva	Internetová vrstva
Spojová vrstva	Vrstva síťového rozhraní
Fyzická vrstva	

Tabulka 2.1 – Porovnání ISO/OSI a TCP/IP modelu
Zdroj: Spurná, 2010 (vlastní zpracování)

2.6.Ethernet

První využití se datuje od 70. let 20. století. Je to technologie používaná v sítích LAN a je definována pomocí standardů 802.2 a 802.3. V ISO/OSI modelu se Ethernet nachází ve spodních dvou vrstvách, a to fyzické a spojovací vrstvě. Rámce Ethernetu musí obsahovat zdrojovou a cílovou MAC adresu, protože se data posílají prostřednictvím sdíleného média pomocí metody CSMA/CD (Spurná, 2010).

Nejstarší varianty Ethernetu jsou 10Base-5, 10Base-2, 10Base-T, 10Base-F. Rychlost, se kterou standard pracuje, je udána v první číslici, slovo Base označuje signalizační metodu a jako poslední v názvu je písmeno, které označuje typ kabelu. Optický kabel je označen písmenem F a nestíněná kroucená dvoulinka je označena písmenem T.

Prostřednictvím standardu 802.3 rozdělujeme Ethernet do několika variant. Jako přenosové médium tyto varianty využívají optické, nebo metalické kabely (Spurná, 2010). Níže budou popsány jeho novější varianty a v Tabulce 2.2 lze vidět souhrn nejrozšířenějších variant Ethernetu a jejich nejdůležitější specifikace.

2.6.1. Fast Ethernet

Šířka pásma Fast Ethernetu je 100 Mb/s a k přenosu dat nejčastěji využívá kabel UTP, či optické vlákno. Na rozdíl od Ethernetu není možné využít koaxiální kabel. Při využití kabelu UTP musí být kategorie 5 a vyšší. Vysílá se jiným párem vodičů a jiným se signál přijímá. Vodičem číslo 1 a 2 se signál vysílá a vodiči číslo 3 a 6 se přijímá. Je založen na metodě náhodného přístupu CSMA/CD. Varianty Fast Ethernetu jsou 100Base-TX, 100Base-FX a další (Trulove, 2009).

2.6.2. Gigabit Ethernet

Šířka tohoto typu Ethernetu je 1 000 Mb/s (1 Gb/s), musí mít dobré načasování, synchronizaci i přesnou interpretaci signálu na vzdáleném konci média. Všechny tyto vlastnosti jsou důležité a je na ně kladen velký důraz proto, že se data na přenosové lince zdržují opravdu krátkou dobu. Také kódování je důležité a musí být komplexnější než u jiných typů, data jsou totiž náchylnější k rušení. K přenosu se opět používá kabel UTP a optické vlákno. Při využití UTP kabelu se používají všechny čtyři páry a kabel musí být kategorie 5 a vyšší. Provoz je full-duplexní. Varianty Gigabitového Ethernetu jsou 1 000Base-T, 1 000Base-TX, 1 000Base-SX a 1 000Base-LX (Trulove, 2009).

2.6.3. 2,5/5 Gb Ethernet

Organizace IEEE nově schválila Ethernet se šířkou pásma 2,5 Gb, který využívá UTP kabel kategorie 5e, což je nejlevnější kabeláž, kterou lze při drátových přenosech využít. Tato varianta má označení 2,5GBase-T, využívá full-duplexové vysílání a má maximální dosah na 100 metrů.

Dalším novým přírůstkem do technologie Ethernetu je 5 Gb Ethernet. Parametry má podobné jako 2,5 Gb, také využívá full-duplexové vysílání s maximálním dosahem na 100 metrů, ale využívá UTP kabel kategorie 6. Tento typ kabeláže obsahuje vyztužené kroucení, proto je také odolnější vůči rušení a přeslechům. Tato varianta nese označení 5GBase-T. (Network World, 2016)

2.6.4. 10 Gb Ethernet

Šířka tohoto pásma je 10 Gb/s a je nejrychlejší verzí Ethernetu, pro přenos se využívá hlavně optické vlákno. Tato technologie se využívá pro zvýšení přenosové rychlosti u stávajících sítí a zařízení. Zvýšit rychlost přenosu zařízení je možné, protože formát rámce tohoto Ethernetu je slučitelný se staršími verzemi. Tento typ lze použít na sítích LAN, anebo je také možné jej použít na vzdálená spojení sítí MAN nebo WAN. Je povoleno pouze full-duplexní vysílání. Varianty 10 Gigového Ethernetu jsou 10GBase-CX4, 10GBase-T, 10GBase-SX4 a 10GBase-LX4 a další (Spurná, 2010).

2.6.5. Způsob komunikace

Full-duplex

Díky provozu full-duplex, můžou oba uzly na lince typu point-to-point data, jak vysílat, tak přijímat. Využívá se u spojení počítače a přepínače, spojení dvou přepínačů, anebo spojení dvou počítačů, a to křížovým kabelem (Trulove, 2009).

Half-duplex

Jak plyne z názvu, jde vlastně o poloviční provoz. V danou chvíli umožní jednomu zařízení jen vysílat a druhému jen přijímat data. Takže pokud chce začít vysílat druhý uzel, musí počkat, až skončí vysílání prvního uzlu.

Před tím, než začnou zařízení vysílat, musí se pomocí spojové vrstvy dohodnout, jaký typ vysílání budou používat. Pokud jedno ze zařízení nedokáže používat full-duplex provoz, jsou nuceni používat half-duplex. Jestliže full-duplex vyhovuje oběma, používají jej (Trulove, 2009).

Šířka pásma	Označení	Typ vysílání	Přenosové médium	Maximální vzdálenost
10 Mb/s	10Base-5	Half-duplex	Tlustý koaxiální kabel	500 m
10 Mb/s	10Base-2	Half-duplex	Tenký koaxiální kabel	185 m
10 Mb/s	10Base-T	Half-duplex	UTP kabel od kategorie 3	100 m
100 Mb/s	100Base-T	Half-duplex	UTP kabel od kategorie 5	100 m
200 Mb/s	100Base-TX	Full-duplex	UTP kabel od kategorie 5	100 m
100 Mb/s	100Base-FX	Half-duplex	Mnohovidové optické vlákno	400 m
200 Mb/s	100Base-FX	Full-duplex	Mnohovidové optické vlákno	2 km
1 Gb/s	1 000Base-T	Full-duplex	UTP kabel kategorie 5e	100 m
1 Gb/s	1 000Base-TX	Full-duplex	UTP kabel kategorie 6	100 m
1 Gb/s	1 000Base-SX	Full-duplex	Mnohovidové optické vlákno	550 m
1 Gb/s	1 000Base-LX	Full-duplex	Jednovidové optické vlákno	5 km
2,5 Gb/s	2,5GBase-T	Full-duplex	UTP kabel kategorie 5e	100 m
5 Gb/s	5GBase-T	Full-duplex	UTP kabel kategorie 6	100 m
10 Gb/s	10GBase-CX4	Full-duplex	Twinaxial – kabel podobný koaxiálnímu kabelu, obsahuje místo jednoho vnitřního vodiče dva	15 m
10 Gb/s	10GBase-T	Full-duplex	UTP kabel kategorie 6a nebo 7	100 m
10 Gb/s	10GBase-SX4	Full-duplex	Mnohovidové optické vlákno	300 m
10 Gb/s	10GBase-LX4	Full-duplex	Jednovidové optické vlákno	10 km
25 Gb/s	25GBase-T	Full-duplex	UTP kabel kategorie 8	30 m
40 Gb/s	40GBase-T	Full-duplex	UTP kabel kategorie 8	30 m

Tabulka 2.2 – Nejrozšířenější varianty Ethernetu a jejich specifikace
Zdroj: Spurná, 2010 (vlastní zpracování)

2.7.Bezdrátové sítě

K přenosu dat se využívá mimo metalických a optických kabelů také vzduch. Toto přenosové médium je právě využito u bezdrátových sítí. Výhodou u takto vytvářených sítí je, že není třeba řešit, kudy povede signál. Ten je ovlivněn pouze vysílacím výkonem zařízení a jeho antény. Bezdrátové sítě využívají pro svůj přenos licenční i bez licenční pásmo. Rozlišují se čtyři základní typy bezdrátových sítí (Tanenbaum, 2010).

2.7.1. Přístupový bod

Přístupový bod (Access Point – AP), jinak nazývaný také jako hotspot, je uzlem bezdrátové sítě a je kombinací vysílače a přijímače. AP dokáže propojit kabelovou síť

a bezdrátovou, nebo dva AP mezi sebou. Pokud se propojí dva přístupové body, bezdrátová síť se rozšíří (Tanenbaum, 2010).

2.7.2. Standard 802.11

Snad nejpoužívanější technologií tvořící bezdrátové sítě je Wi-Fi. Ta je standardem IEEE 802.11. Zprvu měla Wi-Fi zajistit bezdrátové propojení zařízení do sítí LAN (Wireless Local Area Network), avšak pomocí hotspotů (přístupových bodů) se postupně začala využívat i k připojení k Internetu. Wi-Fi patří do bezlicenčního, veřejného pásma. Souhrn standardů, pásem, v kterých pracují a jejich teoretické maximální rychlosti lze vidět v Tabulce 2.3.

Standard	Pásmo	Teoretická maximální rychlost [Mb/s]
802.11 a	5	54
802.11 b	2,4	11
802.11 g	2,4	54
802.11 n	2,4 nebo 5	600
802.11 ac	2,4 a 5	1 000
802.11 ad	2,4; 5; 60	7 000

Tabulka 2.3 - Standardy IEEE 802.11

Zdroj: Horák, Keršláger, 2011 (vlastní zpracování)

Standard 802.15

Tento standart je nazýván WPAN (Wireless Personal Area Network), nebo také jako Bluetooth a slouží k bezdrátovému spojení dvou zařízení na vzdálenost 1-100 metrů.

Standard 802.16

Standardem 802.16 nazýváme WiMAX (Worldwide Interoperability for Microwave Access). WiMAX je stále se rozvíjející širokopásmovou technologií, stejně jako Wi-Fi má přístup do celosvětové sítě Internet. Je zaměřena na venkovní sítě a je doplňkem Wi-Fi.

Standard GSM

Tento standard GSM (Global Systém for Mobile Communication) je určený pro mobilní telefony a má na starost digitální přenos hovoru a SMS zpráv. Využívá

protokol, který slouží pro přenos dat v síti, a to protokol GPRS. Dosah standardu bývá od stovek metrů až po desítky kilometrů a je závislý na výkonu antény (Spurná, 2010).

Existují mobilní sítě několika generací. Druhá generace 2G, do které spadá standard GSM, přenáší data rychlostí 9,6 kb/s.

Přechodová generace mezi druhou a třetí je 2,5G. Tato generace rozšiřující GSM pracuje s přepínáním packetů a umožňuje tím přenos dat rychlostí od 115 do 384 kb/s. V praxi se můžeme setkat také s technologií GPRS a EDGE (2,75G).

Další generací je již zmíněná 3G. Do této generace patří například UMTS a jeho hlavním přínosem je podpora kvality služeb (QoS), rychlost přenosu dat je až 3,1 Mb/s.

Do přechodové generace 3,5G (HSDPA) spadá GSM a UMTS systém s rychlostí přenosu dat až 14 Mb/s, rychlost přenosu dat 3,9G (LTE) dosahuje až 326 Mb/s.

Výhodou čtvrté generace 4G – LTE-Advanced oproti LTE (3,9G) je, že splňuje požadavky Mezinárodní telekomunikační unie na mobilní sítě čtvrté generace. Tudíž má přenosovou rychlost nad 1 Gb/s u statického zařízení a 100 Mb/s u velmi rychle se pohybujícího mobilního přístroje. I když je rychlost připojení mnohonásobně rychlejší než přes xDSL, tak toto „mobilní“ připojení k internetu je v dnešní době ještě uměle omezováno pomocí maximálního množství stažených dat (*3GPP, 2013).*

2.7.3. Zabezpečení

Zabezpečení bezdrátových sítí není radno podceňovat. Bezdrátové sítě musí být zabezpečeny proti potenciálním útočníkům. Těm totiž stačí být pouze v dosahu vysílaného signálu na rozdíl od metalických sítí, u kterých je vyžadován fyzický přístup k médiu, takže pokud se někdo nedostane ke kabelu a nepřipojí se kabelem do sítě, jsou data v bezpečí. Zabezpečení bezdrátových sítí lze rozdělit do dvou základních skupin (Tanenbaum, 2010).

Šifrování sítě

První skupinou je šifrování provozu sítě, které zajišťuje zabezpečení bezdrátové sítě. Pokud uživatel nezná přístupové heslo, není schopen odposlouchávat komunikaci probíhající právě na bezdrátové síti. K tomuto šifrování jsou nejčastěji využívány metody WEP, WPA a WPA2.

Další skupinou a způsobem zabezpečení může být autorizační opatření, které řídí přístup oprávněných uživatelů do sítě. V tomto případě se využívá mimo jiné kontrola MAC adres. Metoda má ale nízkou spolehlivost, proto se využívají také již uvedené metody WPA, WPA2 nebo RADIUS server (ověřování přihlašovacím jménem a heslem) (Tanenbaum, 2010).

Kontrola MAC adres

MAC adresy jsou ověřovány podle seznamu, na kterém jsou povolené MAC adresy. Tyto adresy mohou danou síť používat. Tato tabulka MAC adres je uložena na přístupovém bodě, přístupový bod si po ověření řídí provoz samo. MAC adresa se dá na síťových zařízeních měnit a útočník může mít MAC adresu odpovídající některé z tabulky, a tak se vydávat za věrohodného klienta. Proto není metoda kontrol MAC adres příliš spolehlivá (Sosinsky, 2010).

Zablokování vysílání SSID

Zabezpečení pomocí zablokování vysílání SSID (Service Set Indentifier) je nejjednodušší cestou, jak síť zabezpečit. Cílem je znemožnění viditelnosti přístupového bodu zablokováním vysílání broadcastu se SSID. Výsledkem je situace, kdy se běžným uživatelům nezobrazí síť v dostupných bezdrátových sítích vyhledávaných na počítači. Ale jakmile se útočník začne připojovat k přístupovému bodu, jehož připojování je v otevřené podobě, SSID může odposlouchávat (Tanenbaum, 2010).

WEP

Toto zabezpečení spoléhá na systém sdílených klíčů. Jsou zadány statické WEP klíče, které jsou dostupné koncovým bodům, a to na přístupovém bodě i na straně klienta. K WEP klíčům je ale velice jednoduchá dostupnost a šifrování tak zajišťuje velmi slabou úroveň ochrany, proto je mnohem vhodnější metoda WPA. Pokud se útočník dostane k určitým rámcům a analyzuje je, dostane klíč. V dnešní době dokonce existuje řada programů pro získávání WEP klíčů (Sosinsky, 2010).

WPA

Metoda šifrování WPA využívá WEP klíčů, řeší ale problémy protokolu tím, že zavádí generování klíčů mechanismem TKIP (Temporary Key Integrity Protocol – protokol dočasné integrity klíčů). Pomocí TKIP je vygenerován pro každý přenášený paket nový klíč (na rozdíl od WEP, který používá pro všechny pakety stejný klíč). Přístupový bod

i strana klienta má předem určený sdílený klíč, který je stejný na obou stranách. Tato autentizace přístupu do WPA je provedena pomocí PSK (Pre-Shared Key), anebo RADIUS serverem. WPA je proto mnoho bezpečnější díky delším klíčům a také kvůli tomu, že se šifrovací klíče neustále mění (Sosinsky, 2010).

WPA2

Novějším modelem WPA je WPA2, který je kvalitnější a bezpečnější, ale pro své využití vyžaduje větší výpočetní výkon. Všechna zařízení, která splňují normu pro WPA2 jsou z povinnosti označeny obchodní známkou a logem Wi-Fi. K šifrování využívá AES (Advanced Encryption Standard – pokročilý šifrovací standard). Technologii WPA2 není možno využívat u starších zařízení, která nerozumí protokolu TKIP, AES anebo jejich kombinaci (Sosinsky, 2010).

2.8.Síťový hardware – aktivní prvky sítě

V této kapitole jsou definovány a popsány základní aktivní hardwarové prvky nezbytné pro funkčnost počítačové sítě. Mezi aktivní prvky sítě patří například zesilovač, jehož funkce je v této práci pouze nastíněna. Pro naše potřeby je důležitý hlavně switch a router. Tyto prvky jsou proto popsány více konkrétně.

2.8.1. Repeater

Jelikož signál ztrácí kvalitu a správnou koordinaci při příliš velké vzdálenosti, může být podpořen právě repeatrem (zesilovačem), který rozšiřuje (zesiluje) dosah signálu (Sosinsky, 2010).

2.8.2. Switch

Switch (přepínač) spojuje dvě sítě na jedné nebo více vrstvách síťového modelu OSI. Principem switche je oddělování komunikujícího počítače od zbytku sítě a vytvoří tak vlastně virtuální okruh mezi počítači. Výhodou je, že nedochází ke zpomalování sítě, protože komunikující počítače nejsou zahlcovány cizími pakety a výměna dat mezi koncovými počítači tak probíhá maximální rychlostí. Switch má řadu vlastností, na které je třeba si dát pozor při jeho výběru. Ovlivňuje ho například počet portů, jejich zrcadlení nebo schopnost přidělovat jim priority. Velmi důležitá je také nominální rychlost portů, duplexní operace ovlivňující propustnost přepínače, nebo agregace. To znamená schopnost zasílat data přes více spojení zároveň, a to stejnému koncovému počítači.

Dalším důležitým aspektem je filtrování (např. filtrace podle MAC adres) (Horák, Keršláger, 2011; Sosinsky, 2010).

2.8.3. Router

Router, jinak zvaný směrovač, je takové zařízení v síti, které zajišťuje propojení nejméně dvou různých sítí. Jednou z jeho funkcí je rozdělování kolizních domén, dále také filtruje a blokuje všesměrové vysílání. Mimo jiné se může starat o funkci DHCP serveru a překlad síťových adres (NAT). Další jeho funkcí je zajištění optimální trasy pro směrování paketů k cíli. Výkonné routery zpracovávají vysokou míru dat, proto jsou to vlastně velmi silné počítače.

Už od svého počátku bylo toto logické zařízení založeno na konceptu více síťových rozhraní. Router je daný dvěma oddělenými funkčními systémy. Jedním z nich je řídící úroveň (Control Plane) a druhou je doručovací úroveň (Forwarding Plane).

Řídící úroveň rozhoduje o portu, přes který budou doručeny k cíli pakety a zahrnuje funkce filtrace, blokování a zajištění kvality služby (Quality of Service – QoS) na základě protokolů zahrnuté výrobcem do směrovače.

Doručovací úroveň se stará o přijetí paketů a o to, aby byly odeslány prostřednictvím vybraného rozhraní. Na vstupním rozhraní pakety vlastně prověřuje a poté je přenáší na správné odchozí rozhraní (Sosinsky, 2010).

Funkce routeru

NAT – Network Address Translation

NAT slouží k překládání interní privátní adresy a veřejné adresy. K překladu adres musí dojít, pokud chce počítač v interní privátní síti přistupovat ke zdrojům na veřejné síti, například na internet. Tento překlad adres probíhá na hraničním zařízení, kterým je tedy většinou směrovač. Probíhá to tak, že počítač vyšle dotaz směřovaný na vnější zařízení umístěné na internetu. Hraniční směrovač musí odstranit problém, kdy se v posílaných datech nesmí vyskytovat jako odchozí IP adresa privátní adresa počítače. Hraniční směrovač tedy musí zajistit, aby se takto nedělo, protože odpověď na tento dotaz by nebyla v síti Internet směrována a pakety s privátní adresou cíle by byly zahozeny. Proto směrovač nahradí zdrojovou privátní adresu veřejnou IP adresou, tato adresa je již v síti Internet směrovatelná. Směrovač půjčuje a zaměňuje privátní adresy v komunikaci za veřejné. Veřejnou IP adresu může mít k dispozici jednu, nebo i větší počet. K dispozici

má veřejných IP adres obvykle méně než privátních IP adres ve své privátní síti. Pak musí jednotlivé komunikace odlišit, musí jim tedy přidělit porty (NAT s podporou PAT – Port Address Translation). Komunikace, která je odchozí a přicházející odpovědi z veřejné sítě je mapována pomocí čísel portů. Toto mapování je důležité pro směrovač, který podle těchto čísel dokáže odlišit a rozhodnout, kterému počítači, kterou odpověď poslat (Spurná, 2010).

2.9.Síťový hardware - pasivní prvky sítě

2.9.1. Strukturovaná kabeláž

Tato kapitola obsahuje popisy pasivních prvků sítě, jak optického kabele, tak metalických kabelů, konkrétně je zmíněn koaxiální kabel a kroucená dvojlinka, které je věnován podrobnější popis (Horák, Keršláger, 2011).

Optický kabel

Optický kabel již není založen na principu metalických kabelů, nýbrž na přenášení světelných impulsů ve světlovodivých optických vláknech. Tato vlákna jsou tenká a flexibilní média. V kabelu jsou minimálně dvě vlákna, pro každý směr je určeno jedno. Ale běžně jich bývá v kabelu několik párů (Horák, Keršláger, 2011; Kurose, Ross, 2014).

Koaxiální kabel

Jedním z pasivních prvků sítě je také koaxiální kabel, který se nejvíce používá v kabelových televizních systémech (Kurose, Ross, 2014).

Kroucená dvojlinka

Kroucená dvojlinka (Twisted Pair Cable) je odvozena od telefonního kabelu a u telefonních sítí se používá již přes sto let. Je to nejlevnější a nejčastější metalický vodič a nejvíce používané přenosové médium v sítích LAN. Skládá se z osmi vodičů tvořících čtyři páry a jsou uspořádány v pravidelné spirále. Vodiče přenášejí elektrický signál a ten je náchylný na rušení. Toto elektrické rušení vzniká vzájemným působením ostatních vodičů. Proto jsou vodiče zkrouceny do spirály, která působí jako ochrana právě proti tomuto elektrickému rušení, protože zkroucení vodičů zapříčiní pravidelné střídání jejich vzájemné polohy. Tím se minimalizuje ovlivňování jednoho vodiče druhým a jejich vzájemné vlivy (Horák, Keršláger, 2011; Kurose, Ross, 2014).

Existují dvě provedení kroucených dvojlinek, nestíněná kroucená dvojlinka (UTP) a stíněná kroucená dvojlinka (STP) (Horák, Keršláger, 2011).

Nestíněná kroucená dvojlinka (UTP – Unshielded Twisted Pair) spočívá v uložení jednotlivých párů do vnější plastické izolace bez dalšího zabezpečení, což lze vidět na Obrázku 2.1. Používá se nejčastěji u počítačových sítí v budovách, což znamená v síti LAN (Horák, Keršláger, 2011; Kurose, Ross, 2014).

Obrázek 2.1 - UTP kabel
Zdroj: Khcn Cinet, 2017

Stíněná kroucená dvojlinka (STP – Shielded Twisted Pair) má na rozdíl od UTP zvýšenou ochranu. K té přispívá kovové opletení (stínění), které může stínit každý pár uvnitř kabelu (Obrázek 2.2) anebo jen plášť kabelu (ScTP – Screened Twisted Pair – Obrázek 2.3). Každopádně tento druh kroucené dvojlinky je samozřejmě dražší než UTP a bývá využit v případech, kdy dochází k vnějšímu rušení (Horák, Keršláger, 2011).

Obrázek 2.2 - STP
Zdroj: Khcn Cinet, 2017

Obrázek 2.3 – ScTP kabel
Zdroj: Khcn Cinet, 2017

2.9.2. Konektory

RJ-45

V počítačových sítích je nejrozšířenějším konektorem právě RJ-45 (používá se pro zapojení síťových kabelů UTP a STP) a lze ho vidět na Obrázku 2.4. Tento konektor má osm kontaktů. Při standardu 1 000Base-T se využívá všech osmi kontaktů (čtyři páry kontaktů) (Horák, Keršláger, 2011).

Obrázek 2.4 - Konektor RJ-45
Zdroj: Pinterest, 2017

RJ-11

Konektor RJ-11 je předchůdcem RJ-45, pro jeho nekompatibilitu s moderními počítači už se však používá pouze pro telefonní přípojky. Na škodu je totiž jiný tvar konektoru a počet vodičů, což lze vidět na Obrázku 2.5. Tento konektor má čtyři vodiče, používá se při navázání spojení telefonní linky (Horák, Keršláger, 2011).

Obrázek 2.5 - Konektor RJ-11
Zdroj: Pinterest, 2017

2.10. Server obecně

Server je obecně označován jako počítač, který poskytuje nějaké služby, nebo jako počítačový program, který tyto poskytované služby realizuje. Již zmíněné služby jsou poskytovány klientům, tento proces se nazývá model klient-server, buď jednomu počítači (lokálně) nebo více počítačům za pomoci počítačové sítě (síťové služby).

Například taková obsluha připojené tiskárny, nebo správa automatických aktualizací může být službou lokální. A sdílení disků, tiskáren, nebo schopnost ověřit uživatele podle jména a hesla (autentizace) a podobně, můžou být služby poskytované serverem v lokální síti (LAN). V síti Internet či jiných větších sítích servery uchovávají a nabízejí webové stránky a poskytují další služby, například DNS nebo e-mail.

Softwarový server komunikuje s klientem pomocí definovaného protokolu, v Microsoft Windows se využívá SMB pro sdílení disků a tiskáren nebo HTTP pro webový server. Server je rozlišován na dva typy, a to podle toho, jestli je server vyhrazen jen pro poskytování služeb nebo může sloužit i uživatelům. Server tedy rozlišujeme

na dedikovaný, který je právě vyhrazen pro speciální účely, bez přímého přístupu uživatelů. A dalším typem je nededikovaný server, který slouží uživateli zároveň jako obyčejný počítač (Tanenbaum, 2010).

2.10.1. NAS server – Network Attached Storage

Jak vyplývá z názvu, toto datové úložiště využívá ke svému účelu síť, mimo to je také připojené k místní síti LAN. Úložištěm NAS tedy může být server nebo dedikované zařízení, které obsahuje jeden nebo více disků. NAS je užitečný jak pro svou jednoduchou konfiguraci, tak pro sdílení dat bez zbytečných nastavování sdílení disků a přístupových práv, na rozdíl od ukládání na běžném počítači. Pokud má NAS server více disků, umožňuje zapojení disků do softwarového RAID pole. Pro toto zapojení je typická nízká spotřeba a kompaktní velikost, to však v závislosti na počtu disků. NAS server ovšem poskytuje i jiné služby jako jsou například HTTP server, FTP server nebo Print server. Tyto služby jsou nastavovány formou webového rozhraní (Tanenbaum, 2010).

2.11. RAID – Redundant Array of Independent Disks

RAID (v překladu vícenásobné diskové pole nezávislých disků) jsou typy diskových řadičů, nebo speciálního softwaru. Ty zajišťují zabezpečení koordinované práce dvou, nebo více fyzických diskových jednotek, a to za pomoci určitých speciálních funkcí. Výhodou je tak zvýšení výkonu a odolnosti vůči chybám, nebo ztrátě dat v závislosti na typu těchto polí. Existuje několik typů RAID – RAID 0, RAID 1, RAID 3, RAID 5 a další, které nejsou tak často využívány (Tanenbaum, 2010).

3 Analýza současného stavu počítačové sítě a prostředí

V této kapitole bude popsána charakteristika společnosti EXTRAVÝFUK, s. r. o. a analyzován současný stav počítačové sítě, včetně připojení do sítě internet, hardwarového a softwarového vybavení společnosti a prostředí, ve kterém se společnost nachází.

3.1.Charakteristika společnosti

Společnost EXTRAVÝFUK, s. r. o. vznikla 25. 3. 1996 zapsáním do obchodního rejstříku vedeného u Krajského soudu v Ostravě oddíl C, vložka 14422. Společnost má nyní sídlo v obci Dobrá u Frýdku-Místku na adrese Dobrá 153, kde se přestěhovala v roce 2006 kvůli neustálému nárůstu poptávky po zboží, s kterým obchoduje jak z řad maloobchodu, tak i velkoobchodu. V roce 2010 byl hlavní sklad a kanceláře firmy přestěhovány na adresu Příborská 1001, PSČ 738 01, Frýdek-Místek a v roce 2012 byla firma rozšířena o skladové prostory v Praze na adrese Františka Diviše 1275/1a, Praha 10 – Uhříněves, PSČ 104 00 kvůli posílení velkoobchodu na území hlavního města Prahy, kde sídlí většina celorepublikových firem, které jsou hlavními velkoodběrateli společnosti.

Hlavním předmětem podnikání společnosti je koupě zboží za účelem jeho dalšího prodeje, a to hlavně prodej výfuků, katalyzátorů, filtrů DPF, pružných dílů a nejrůznějších doplňků k tomuto zboží.

3.1.1. Základní údaje o firmě

Datum zápisu: 25. 3. 1996

Obchodní firma: EXTRAVÝFUK, s. r. o.

Sídlo: Dobrá 153, Dobrá u Frýdku-Místku, PSČ 739 51

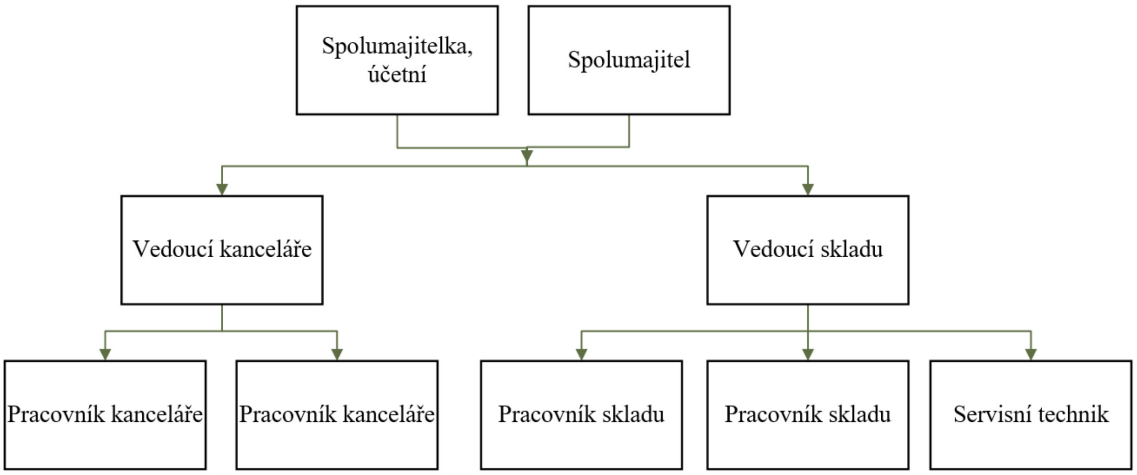
Identifikační číslo (IČO): 646 199 58

Daňové identifikační číslo (DIČ): CZ646 199 58

Právní forma: Společnost s ručením omezeným

3.1.2. Organizační struktura

Obchodní firma má dva spolumajitele, a to Pavla Šebestu a Martinu Šebestovou, která je zároveň účetní firmy. Pod sebou mají dva hlavní vedoucí, a to prvního, který má na starost celou kancelář firmy, kde se zpracovávají objednávky, poptávky, faktury, tvoří se štítky na balíky pro přepravní společnost PPL a mají na starost kontakt se zákazníky, jako je vyřizování telefonických hovorů, e-mailů včetně domlouvání montáže. Druhý je vedoucí skladu, kde se naskladňuje od dodavatelů zboží, vyskladňuje pro velkoobchodní odběratele i maloobchodní objednávky (E-shop, nákup na prodejně, telefonické objednávky), probíhá balení zboží do kartonových krabic pro přepravní službu, a nakonec se provádí montáž dílů. Celou organizační strukturu firmy lze vidět na Obrázku 3.1.

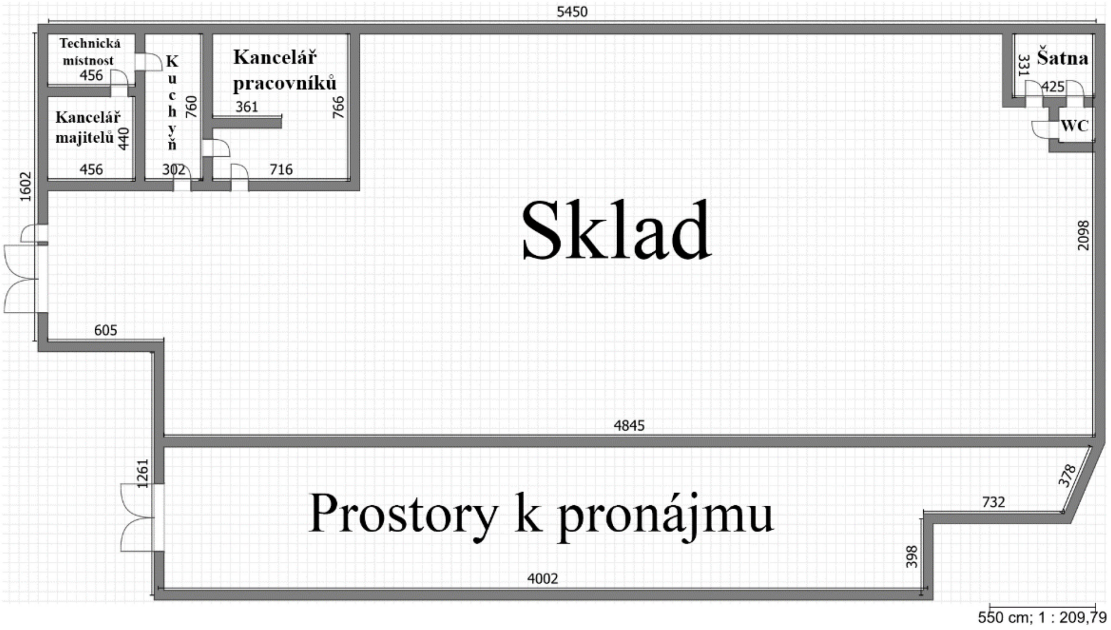


Obrázek 3.1 – Organizační struktura

Zdroj: vlastní

3.2.Analýza prostředí

Pobočka ve Frýdku-Místku se nachází na adrese Příborská 1001, PSČ 738 01, Frýdek-Místek. Jedná se o rozsáhlou jednopodlažní budovu ve vlastnictví společnosti se skladovacími prostory včetně kancelářských místností a různých společných prostor jako kuchyň, šatny a sociální zařízení o celkové výměře 1514 m^2. V budově se také nachází prostory, které jsou nyní rekonstruovány, a společnost plánuje tyto prostory pronajímat. Pro vypracování návrhu počítačové sítě byl zpracován půdorys budovy včetně rozmístění jednotlivých místností, který vidíte na Obrázku 3.2.



Obrázek 3.2 - Půdorys budovy

Zdroj: vlastní

3.3.Analýza počítačové sítě

Samotná počítačová sít i veškeré hardwarové a softwarové vybavení společnosti bylo zakoupeno, nainstalováno a uvedeno do provozu před více než 6 lety, to je s ohledem rychlého technologického vývoje v odvětví IT a každým rokem zvyšující se riziko selhání jednotlivých hardwarových prvků pro firmu již neakceptovatelné. Proto se společnost rozhodla kompletně modernizovat IT infrastrukturu a vylepšit tím spolehlivost, propustnost a zabezpečení počítačové sítě a díky této modernizaci implementovat prvky jako zabezpečovací kamerový systém a síťová záloha dat, na které momentálně není síť stavěná a v neposlední řadě zasíťovat prostory k pronájmu, při příležitosti rekonstrukce.

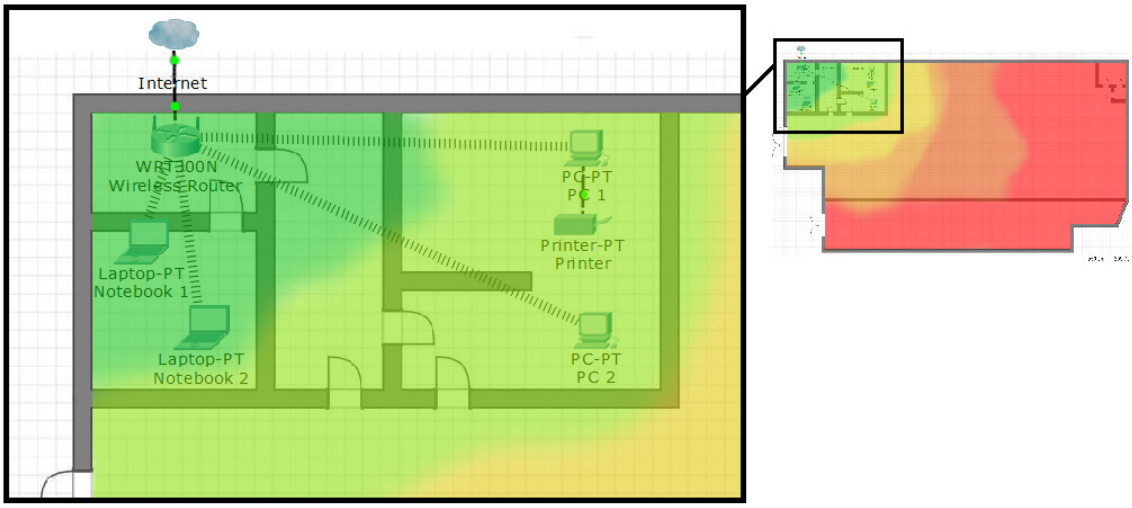
3.3.1. Současná podoba počítačové sítě

Při realizaci sítě v roce 2010 se rozhodla společnost kvůli nenáročnosti jak časové, tak finanční vytvořit počítačovou síť využívající z většiny bezdrátové propojení jednotlivých zařízení. Toto řešení se časem ukázalo jako velice nevhodné kvůli malé propustnosti, spolehlivosti a pokrytí sítě.

V technické místnosti, která je umístěna u kanceláře majitelů, se nachází Wi-Fi router, který je centrální bod celé počítačové sítě a je nejvytíženějším místem sítě. Přes něj je realizováno připojení k internetu, funkce DHCP serveru, DNS serveru, a také bezdrátová část sítě pomocí technologie 802.11g o maximální celkové propustnosti

54 Mbit/s, přes kterou jsou připojeny veškeré notebooky a stolní počítače se systémem Windows a různé přenosné zařízení jako jsou chytré telefony a tablety. Firma nevyužívá a ani neplánuje žádné síťové operační systémy. Dosah bezdrátové sítě dostačuje na pokrytí kanceláře majitelů a pracovníků, ale pokrytí mimo tyto místnosti vesměs neexistuje, což je pro aktuální potřeby firmy již nedostatečné.

Router se nachází na adrese 192.168.1.1 (výchozí brána) a přidělování IP adres funguje automaticky pomocí DHCP serveru, server přiděluje adresy v rozsahu 192.168.1.2 - 192.168.1.254 a tvoří tak jednu velkou síť bez nějakých podsítí (subnetu). Rozmístění zařízení a znázornění fyzického propojení mezi nimi, včetně vyobrazení síly bezdrátové sítě pomocí teplotní mapy je vyobrazeno na Obrázku 3.3.



Obrázek 3.3 – Vyobrazení zařízení a teplotní mapa bezdrátové sítě

Zdroj: vlastní

Zabezpečení bezdrátové sítě je v dnešní době již nedostatečné. Síť pouze s jedním SSID a zabezpečením se šifrováním WEP, která je stejná jak pro majitele, zaměstnance, tak i obchodní partnery, kterým se heslo k bezdrátové síti většinou dává při obchodních jednáních. Zákazníkům se přístup k bezdrátové síti dává jen výjimečně. Tato situace je z dnešního pohledu velice riziková hlavně ohledně zabezpečení citlivých firemních dat, ke kterým by mohl mít přístup kdokoliv jen s průměrnými znalostmi zabezpečení sítě a jejich odposlechu, bez výraznějších problémů s překonáním zabezpečení.

Dalším problémem je řešení připojení tiskárny, která je nyní pevně připojena pomocí USB kabelu ke stolnímu počítači v kanceláři pracovníků a následně sdílena přes síť. Hlavní nevýhodou tohoto připojení je, že funkčnost tiskárny je závislá na funkčnosti stolního počítače.

Zálohování firemně důležitých a citlivých dat je postaveno pouze na řešení využívající sdílenou složku v počítači v kanceláří. Toto řešení je zcela nevyhovující z důvodu malé bezpečnosti dat, jelikož přístup k těmto datům má každý, kdo je připojen k síti a neexistují žádná rozdílná přístupová práva a také stejně jako u tiskárny je nutné mít zapnutý daný počítač.

Současná spolehlivost počítačové sítě

Kvůli návrhu modernizace počítačové sítě byl zpracován přehled nejčastějších poruch, který firmě způsobuje problémy s nedostupností internetu nebo celé lokální sítě, což je pro firmu již neakceptovatelné. Tyto problémy a jejich příčiny jsou sesbírány ze záznamu o poruchách, a lze je vidět v Tabulce 3.1.

Typ	Délka trvání	Příčina	Způsob nápravy	Průměrná doba mezi poruchami
Lokální bezdrátová síť	5 až 10 minut	Zamrznutí routeru	Restartování routeru	3 dny
Na straně ISP	140 minut až 12 hodin	Problém na trase ISP	Čekání na vyřešení u ISP	3 měsíce
Na straně ISP	20 až 90 minut	Meteorologické vlivy	Čekání na zlepšení počasí	5 týdnů

Tabulka 3.1 - Současná spolehlivost počítačové sítě

Zdroj: vlastní

Připojení k internetu

V současné době je společnost na pobočce ve Frýdku-Místku připojena do sítě internet přes místního poskytovatele internetového připojení (ISP) Riomedia, a. s. Tento ISP poskytuje v dané lokalitě pouze bezdrátové připojení k internetu o rychlostech 15/2 Mbit/s. Tato rychlost je pro firmu z většiny hledisek dostatečná s výjimkou zálohování firemních dat a bezpečnostních záznamů mimo pobočku firmy. Tento druh připojení trpí ale na časté výpadky, jak kvůli kvalitě bezdrátového dálkového spoje, tak kvůli náchylnosti spoje na meteorologické vlivy. Proto je nutné pro spolehlivé připojení změnit způsob připojení k internetu.

3.4.Požadavky firmy

Společnost si v návaznosti na analýzu počítačové sítě a po konzultaci určila tyto nejdůležitější požadavky na modernizaci své počítačové sítě:

- spolehlivost, propustnost a bezpečnost lokální sítě LAN a WLAN,
- spolehlivost a propustnost připojení k internetu,
- Wi-Fi s dosahem po celé budově,
- rozšíření připojení k internetu do prostor určených k pronájmu,
- přidání jednoho stolního počítače do skladu,
- připravenost sítě pro další rozšiřování,
- tisk odkudkoliv ve firmě a nezávislost na jakémkoliv PC,
- implementace bezpečnostních kamer,
- uchovávání záběru z kamer po dobu 14 dní a online streamování i mimo lokální síť,
- zálohování dat mimo počítače a přístup k nim i mimo lokální síť a bezpečnost těchto dat.

4 Návrh řešení počítačové sítě

4.1.Návrh připojení k internetu

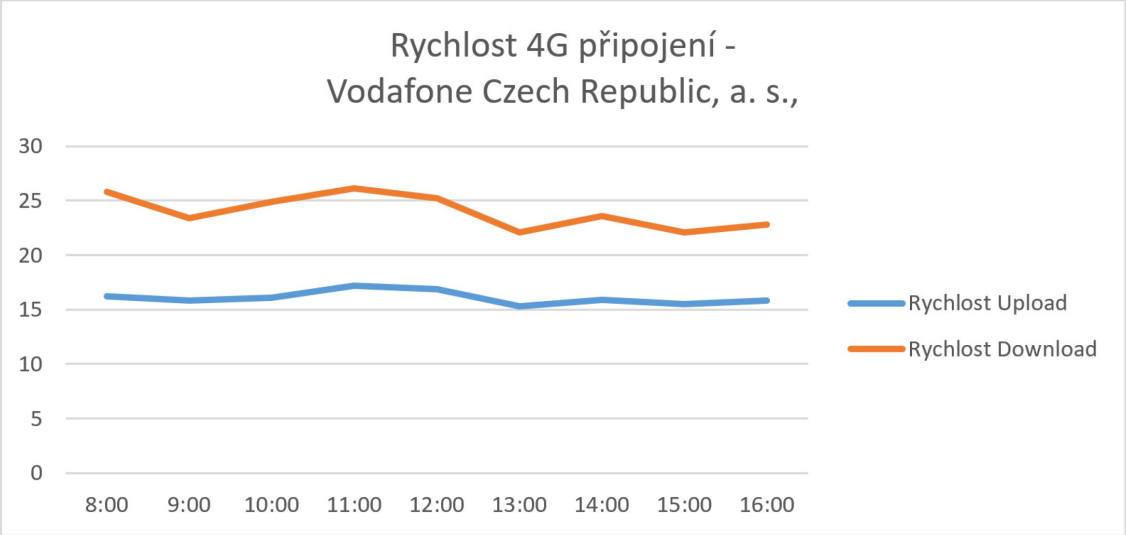
Pro připojení do sítě internet budou využity služby od společnosti Vodafone Czech Republic, a. s., která společnosti poskytuje telekomunikační služby již od roku 2009 v podobě mobilních hlasových a datových služeb pod rámcovou smlouvou. Bude využita technologie VDSL, která využívá metalického vedení v podobě telefonní přípojky, která již v budově je, výhodou bude hlavně spolehlivé připojení, které neovlivňují meteorologické vlivy. Maximální teoretická propustnost bude 20/2 Mbit/s, a možného navyšování rychlosti v průběhu let, jak se budou zavádět nové technologie xDSL, jako je zavedení technologie vectoringu o šířce pásma 17-35 MHz a rychlostech až 80/8 Mbit/s, které se již tento rok bude zavádět. Tak také technologie G.fast o šířce pásma 106 MHz a teoretické propustnosti 250/50 Mbit/s. (CETIN, 2017)

I když je připojení přes kabel pomocí technologie VDSL mnohonásobně spolehlivější než původní bezdrátový spoj, stále jsou ze strany operátora možné méně časté výpadky a pokud se nejedná jen o minutové výpadky, tak již komplikují firmě podnikání. Jako redundantní připojení k sítí internet bude využita technologie 4G, taktéž od společnosti Vodafone Czech Republic, a. s., která má na adrese této pobočky dostupné frekvence 800 MHz, 1 800 MHz a 2 100 MHz o maximální teoretické přenosové rychlosti 75 Mbit/s. Tato možnost byla vybrána z důvodu jednoduché a levné implementace a také minimálních měsíčních nákladu na tuto službu. Firma nyní pod rámcovou smlouvou využívá mobilní připojení pro notebooky a jiné mobilní zařízení, a má mimo jiné i pro data sdílený objem dat ve výši 40 GB. Tento objem dat není firmou využívaný ani z 50 %, a v případě méně častých krátkodobých výpadku bude plně vystačovat pro redundantní připojení.

Dostupnost tohoto připojení byla ověřena na webových stránkách Českého telekomunikačního úřadu a lze vidět na Obrázku 4.1 a poté vyzkoušeno pokrytí včetně dostupných rychlostí v reálním prostředí. Testování probíhalo v průběhu pracovní doby, 4x za hodinu, aby se vyrušilo rozdílné vytížení sítě poskytovatele v průběhu pracovního dne. V Grafu 4.1 vidíte změřené reálné rychlosti v průběhu celého dne.

Obrázek 4.1 - Pokrytí sítě 4G, z leva frekvence: 800 MHz, 1 800 MHz, 2 100 MHz

Zdroj: Český telekomunikační úřad, 2017 (vlastní zpracování)



Graf 4.1 - Reálné rychlosti 4G připojení

Zdroj: vlastní

4.2.Návrh počítačové sítě

S ohledem na analýzu současného stavu počítačové sítě a požadavků, které si firma určila, byla navrhnuta celková změna podoby sítě, která bude využívat pro propojení všech pevných zařízení UTP kabel a pro propojení mobilních zařízení Wi-Fi signálu.

4.2.1. Hardwarové prvky

Z důvodu změny poskytovatele internetového připojení, a hlavně technologie připojení je nutná změna routeru, který se nachází v technické místnosti. Byl vybrán VDSL router od firmy ASUS, a to konkrétně model DSL-AC68U, který již obsahuje mimo jiné VDSL2 modem s podporou nových standardů jako G.993.5 (Vectoring), G.992.1 a G.992.2 (G.Fast), router, switch s 4 portovým Gbit/s LAN, dvoupásmové (2,4 GHz a 5 GHz) Wi-Fi podporující třídy N a AC, možnost záložního 3G/4G připojení, a nakonec VPN server.

Dále pro rozšíření sítě budou využity switche TP-Link TL-SG108PE, které obsahujou 8 portů RJ-45 s rychlostí 1 Gbit/s a podporují standart POE pro napájení dalších menších síťových zařízení a také je managementovatelný.

Pro rozšíření bezdrátové sítě budou využity dvou pásmové (2,4 GHz a 5 GHz) access pointy Asus RP-AC66, které také podporují třídy N a AC, a také je lze připojit k síti bezdrátově, ale v našem případě budou připojeny skrz UTP kabel s konektorem RJ-45, protože toto připojení nesnižuje propustnost sítě na polovinu oproti bezdrátovému připojení.

Počet a cenovou kalkulaci těchto zařízení lze nalézt v Tabulce 4.1.

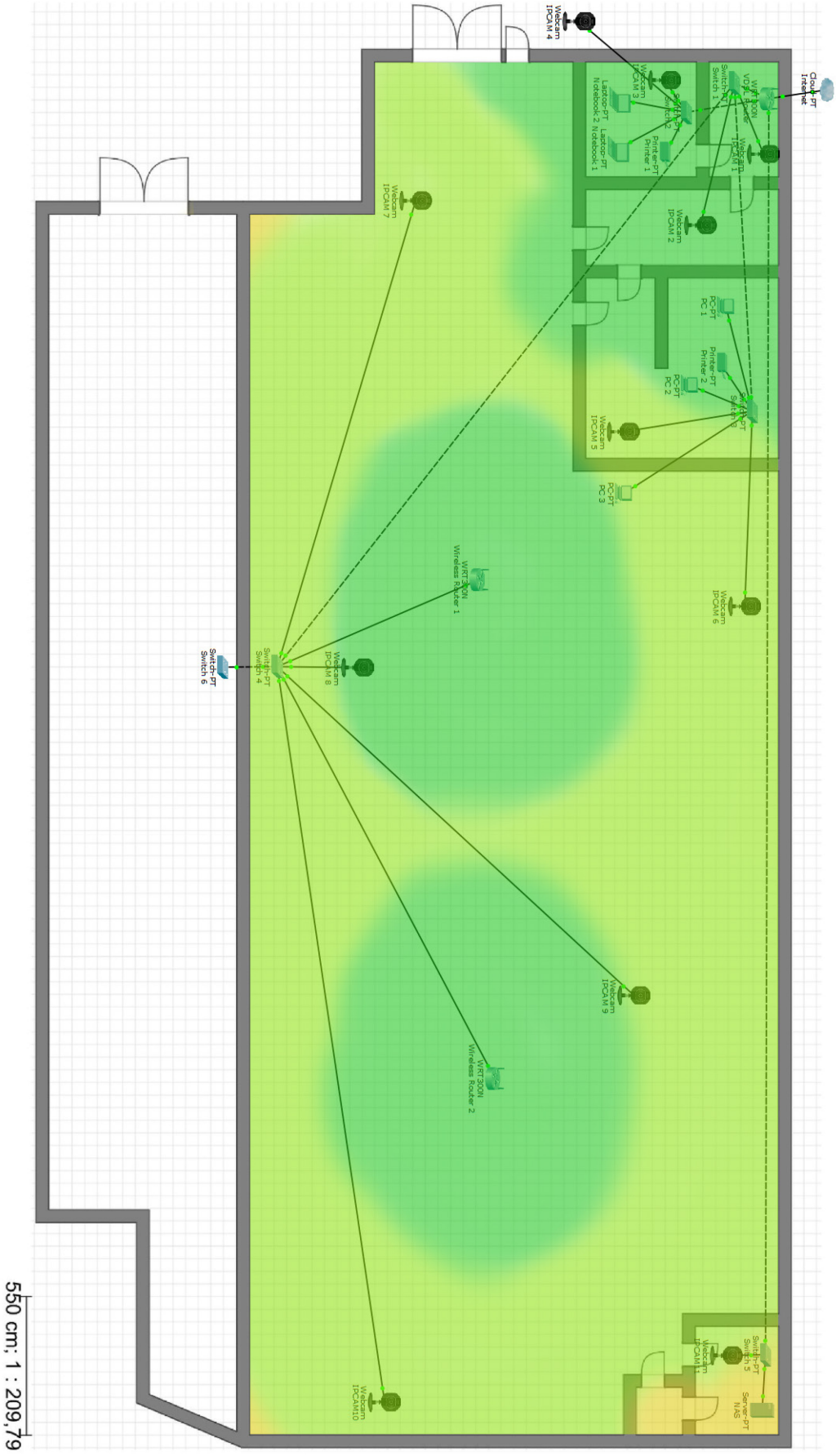
Položka	Počet kusů	Cena za kus bez DPH	Celková cena bez DPH
Asus DSL-AC68U	1	3 800,83 Kč	3 800,83 Kč
TP-Link TL-SG108PE	5	1 643,80 Kč	8 219,00 Kč
Asus RP-AC66	2	2 057,85 Kč	4 115,70 Kč
Celkem	**9**		**16 135,53 Kč**

Tabulka 4.1 - Cenová kalkulace síťových prvků
Zdroj: TINT, s. r. o., 2016 (vlastní zpracování)

Z důvodu propustnosti, spolehlivosti a dosahu sítě budou hlavní prvky sítě propojeny kabelem UTP CAT 6, ve verzi drát pro rozvod ve zdech, kde UTP kabel bude ukončen zásuvkou osazenou na omítce s konektory RJ-45 CAT 6. Pro propojení mezi jednotlivými zařízeními v prostoru bude využit kabel UTP CAT 6 typu lanko zakončený koncovkami RJ-45. Tento kabel UTP CAT 6 je lehce naddimenzován, ale jelikož na rozdíl od aktivního hardwaru má několikanásobně vyšší životnost a bude zabudován v husím krku ve zdech, tak mírně vyšší finanční náklady jsou opodstatněné a v budoucnu nebude problém s výměnou aktivních prvků sítě a díky tomu mnohonásobné zvýšení rychlosti.

4.2.2. Fyzická podoba sítě

Topologie počítačové sítě bude z důvodu rozsáhlosti hvězdicová, co v tomto případě znamená, že téměř do každé místnosti povede z hlavního VDSL routeru UTP kabel a v místnosti bude umístěn switch, na který budou připojeny ostatní zařízení, jako access pointy, notebooky, stolní počítače, tiskárny, síťový disk (NAS) a IP kamery. Rozmístění těchto zařízení a propojení mezi nimi lze vidět na Obrázku 4.2. Tato topologie kvůli své podstatě zásadně snižuje riziko zhroucení celé sítě, když přestane fungovat jedna její část.



Obrázek 4.2 - Fyzická podoba sítě včetně heatmapy bezdrátové sítě

Zdroj: vlastní

Z důvodu bezpečnosti dat v případě požáru, nebo jiných nepříjemných událostí je umístění síťového uložiště co nejdále od všech ostatních prvků. Bohužel internetové připojení neumožňuje plně geograficky rozdílné umístění zálohy dat, například na jiné pobočce firmy. Toto umístění, společně se zamykáním veškerých místností, a nenápadného umístění mimo „centrální dění“ je i dostatečnou ochranou proti zlodějům.

4.2.3. Logická podoba sítě

Pro počítačovou síť firmy bude využita IP adresa sítě třídy C, konkrétně IP adresa 192.1.68.1.0 s maskou podsítě 255.255.255.0. Použitelný rozsah IP adres je od 192.168.1.1 do 192.168.1.254 a adresa broadcastu je 192.168.1.255. Pro jednotlivé aktivní prvky v síti budou určeny pevné IP adresy. První využitelná adresa 192.168.1.1 bude přidělena pro výchozí bránu VDSL routeru. Pro Switche bude přidělen rozsah 192.168.1.2 – 192.168.1.10. Dále pro Access Pointy bude přidělen rozsah IP adres 192.168.1.11 – 192.168.1.15.

Pro zařízení, které budou napojeny na tuto síť (včetně rezerv pro budoucí rozšíření) budou taktéž určeny pevné IP adresy tak, aby již podle IP adresy šlo jednoduše poznat, o které zařízení se jedná, a to konkrétně rozsah od 192.168.1.16 do 192.168.1.35 bude přidělen pro IP kamery, dále rozsah od 192.168.1.36 do 192.168.1.39 pro síťové tiskárny, rozsah od 192.168.1.40 do 192.168.1.41 pro síťové uložiště a nakonec rozsah od 192.168.1.42 do 192.168.1.50 bude určený pro koncové zařízení, jako jsou notebooky a stolní počítače.

Dále všechny mobilní zařízení ve firmě a všechny zařízení napojeny na bezdrátovou síť pro hosty budou mít přidělenou IP adresu z rozsahu 192.168.1.51 až 192.168.1.254, kdy tyto adresy bude přidělovat DHCP server.

4.3. Nastavení počítačové sítě

V této podkapitole bude popsáno nastavení aktivních prvků sítě, jako je DSL router, switch a access point.

4.3.1. Nastavení DSL routeru

WAN

Jelikož je připojení do sítě internet provedeno technologií VDSL2, tak musí být nastaveny přihlašovací údaje, které naleznete v Tabulce 4.2.

Položka v nastavení	Údaj
xDSL modulace	ITU G.993.2
Protokol	PPPoE
Zapouzdření (enkapsulace)	LLC
VLAN mux ID	848
Přihlašovací jméno	VF
Heslo	VF

Tabulka 4.2 - Nastavení DSL routeru

Zdroj: vlastní

Firma disponuje veřejnou pevnou IP adresou, kterou jí poskytl ISP, která má hodnotu 31.30.88.87 a bude tedy adresa WAN portu vždy stejná.

Poté dojde k určení, která síť WAN bude primární a která sekundární. Primární připojení bude nastaveno na port WAN (DSL) a jako sekundární připojení bude sloužit mobilní připojení LTE. Dále bude zapnuta funkce zabezpečující proti selhání připojení k internetu, tzv. Failover Mode, která při výpadku primárního DSL připojení přepne automaticky na sekundární síť WAN, a to LTE připojení. Jakmile bude zase primární síť WAN dostupná, dojde k automatickému přepojení internetového připojení zpět na primární síť WAN, a to díky funkci navrácení služeb pro obnovení, tzv. Allow Failback.

LAN

Nastavení sítě LAN bude takové, že IP adresa výchozí brány (gateway) bude 192.168.1.1 s maskou sítě 255.255.255.0.

DHCP

Dále bude nastavený rozsah, ve které DHCP server přiděluje automaticky adresy připojeným zařízením, nacházejících se v sítí. Tento rozsah bude od 192.168.1.51 do 192.168.1.254. Zbývající rozsah od 192.168.1.2 do 192.168.1.50 bude rezervovaný pro zařízení, které mají nastavenou pevnou IP adresu, a jejich seznam naleznete v Příloze 1.

Bezdrátová síť

Bezdrátová síť je rozšířená pomocí Wi-Fi části DSL routeru, a to jak v pásmu 2,4 GHz, tak také 5GHz pásmu, které nabízí modernější a rychlejší propojení pro novější zařízení.

Bezdrátová síť firmy je složena z celkově čtyř SSID, které jsou viditelné. První dvě SSID, jejichž název je složen z názvu firmy a vysílací frekvence jsou pro zaměstnance a vedení firmy a umožňují plnohodnotný přístup do sítě LAN i internetu. Druhé dvě SSID, které mají přívlastek Host, jsou pro zákazníky a obchodní partnery a tyto dvě SSID jsou odizolované od sítě LAN firmy a umožňují pouze připojení k internetu.

Zabezpečení

Kvůli bezpečnosti sítě bude jako první přenastaveno tovární nastavení pro přihlášení do administrace routeru. Původní nastavení pro uživatelské jméno a heslo bylo admin.

Dále bude nastaven filtr MAC adres pro všechny zařízení, které budou připojeny pomocí pevné sítě, a povolené budou zařízení pouze vlastněné firmou a jejich seznam včetně MAC adres lze vidět v Příloze 1. Všechny ostatní zařízení, které nebudou v tomto seznamu, nebudou moct být připojeny pevným připojením.

Všechny SSID jsou zabezpečeny pomocí šifrování typu WPA2. Výčet SSID, v jakých pásmech pracují, a nastavené heslo lze vidět v Tabulce 4.3, pouze z důvodu bezpečnosti firemní sítě jsou hesla prvních dvou SSID skryté (vyhvězdičkované). Bylo zvoleno heslo o délce 10 znaků, které kombinuje velká a malá písmena, čísla a speciální znaky.

SSID	Pásmo	Heslo
EXTRAVÝFUK, s. r. o. (5 Ghz)	5 Ghz	**********
EXTRAVÝFUK, s. r. o. (2,4 Ghz)	2,4 Ghz	**********
EXTRAVÝFUK, s. r. o. – Host (5 Ghz)	5 Ghz	Extravyfuk1001
EXTRAVÝFUK, s. r. o. – Host (2,4 Ghz)	2,4 Ghz	Extravyfuk1001

Tabulka 4.3 - Seznam SSID

Zdroj: vlastní

NAT

Kvůli přístupu k síťovému uložišti z vnější sítě internet musí být nastaveno překládání síťových adres (NAT) tak, aby bylo možné se k firemním datům a záznamům z kamer dostat odkudkoliv na světě. Hodnoty, které budou nastaveny v administraci routeru lze nalézt v Tabulce 4.4.

Položka	Hodnota
Externí IP adresa	31.30.88.87
Externí číslo portu	5000
Interní IP adresa	192.168.1.40
Interní číslo portu	5000
Protokol	TCP

Tabulka 4.4 - Nastavení NAT

Zdroj: vlastní

4.3.2. Nastavení switche

Jediná změna nastavení, která bude provedena na jednotlivých zařízeních, je změna IP adresy jednotlivého switche. Přiřazení jednotlivých IP adres včetně masek sítě k jednotlivým switchům lze nalézt v Příloze 1.

4.3.3. Nastavení access pointu

Na jednotlivých access pointech bude přenastavená LAN IP adresa včetně masky sítě, její přiřazení lze vidět v Příloze 1. Jelikož v síti již bude jeden DHCP server, tak bude na všech access pointech tato funkce vypnuta.

Zabezpečení

Z důvodu zabezpečení bude taktéž přenastaveno přihlašovací jméno a heslo, kdy původní hodnota byla admin. Z důvodu fyzického nepovoleného připojení budou porty RJ-45 zakázány kromě portu 1, kterým bude zařízení připojeno do sítě LAN.

Bezdrátová síť

Pro rozšíření stávající sítě, bez nutnosti se manuálně nebo automaticky přehlašovat z jedné sítě na druhou bude využito funkce Roaming Assist, díky které nedochází k přerušení spojení při přechodu z dosahu jednoho zařízení ke druhému, protože si jednotlivé zařízení mezi sebou inteligentně předávají dané zařízení. Vysílané SSID budou stejné jako u DSL routeru a jejich seznam naleznete v Tabulce 4.3.

4.4.Návrh koncových zařízení v síti

V této podkapitole se bude zabýváno návrhem koncových zařízení, které budou připojeny do sítě podle požadavků firmy.

4.4.1. IP kamery

Po konzultaci s vedením firmy bylo rozhodnuto, že vzhledem k důvodu pořizování bezpečnostních kamer, který není jen dohled nad zaměstnanci, ale také i pořizování bezpečnostních záznamů i mimo pracovní dobu (v noci) pro případ vloupání či jiných nepříjemných událostí, že bude zvolena IP kamera od firmy Hikvison, konkrétně model DS-2CD2020F-I(W). Hlavní parametry této IP kamery jsou zobrazeny v Tabulce 4.5.

Parametr	Hodnota
Snímací čip	1/2,8" CMOS
Citlivost čipu	0,01 Lux, 0 Lux s IR přísvitem
Maximální rozlišení videa	1920x1080
Snímkovací frekvence při maximálním rozlišení	30 snímku za sekundu
Komprese videa	H.264/MJPEG
Bitrate videa	32Kb/s – 8Mb/s
Max IR přísvit	30 metrů
Úhel záběru	85 °
Počet streamů videa	2
Interface	RJ-45, Wi-Fi
PoE	Ano (802.3af)

Tabulka 4.5 - Parametry vybíraných IP kamer

Zdroj: Hikvision Europe, 2017 (vlastní zpracování)

Počet kusů, které firma bude potřebovat a cenovou kalkulaci lze nalézt v Tabulce 4.6.

Položka	Počet kusů	Cena za kus bez DPH	Celková cena bez DPH
Hikvision DS-2CD2020F-I(W)	11	2 884,30 Kč	31 727,30 Kč
Celkem	**11**		**31 727,30 Kč**

Tabulka 4.6 - Cenová kalkulace IP kamer

Zdroj: (TINT s. r. o., 2016)

4.4.1. Síťové tiskárny

Taktéž po konzultaci s vedením firmy a jejich požadavky mít dvě síťové tiskárny, kdy první bude umístěna v kanceláři vedení, a mimo samotného automatické oboustranného tisku bude umožňovat taktéž automatické kopírování a skenování dokumentů. Z důvodu minimalizování budoucích finančních nákladů na tisk byla zvolena barevná inkoustová tiskárna Epson L655, která místo klasický drahých cartridgů využívá originálního inkoustového tankového systému, díky kterému je následný tisk neporovnatelně levnější.

Jako druhá síťová tiskárna do kanceláře pracovníků byla zvolena černobílá inkoustová tiskárna Epson WorkForce M100, která taktéž využívá tankového systému na černý inkoust.

Cenovou kalkulaci síťových tiskáren lze vidět v Tabulce 4.7.

Položka	Počet kusů	Cena za kus bez DPH	Celková cena bez DPH
Epson L655	1	7 685,12 Kč	7 685,12 Kč
Epson WorkForce M100	1	2 636,36 Kč	2 636,36 Kč
Celkem	**2**		**10 321,48 Kč**

Tabulka 4.7 - Cenová kalkulace síťových tiskáren

Zdroj: TINT s. r. o., 2016 (vlastní zpracování)

4.4.2. Síťové uložiště (NAS)

Jako prvek centrálního zálohování a ukládání dat bude ve firmě sloužit síťové uložiště (NAS), které řeší hlavně původní problém, a to potřebu mít stále zapnutý jeden stolní počítač, na kterém byl sdílený disk, a toto řešení již neodpovídalo požadavkům firmy.

Bylo vybráno zařízení Synology DiskStation DS716+II, které je ideální pro firmu této velikosti i provozu. Obsahuje dva šuplíky pro 3.5" disky, které můžou být spojeny do diskového pole, o výkon se stará 4 jádrový procesor Intel Celeron N3160 o frekvenci 1,6 GHz, kterému sekundují 2 GB RAM. Pro připojení do sítě slouží dva Gbit Ethernetové porty RJ-45 a pro připojení externího disku slouží tři USB verze 3.0. Operačním systémem je DiskStation Manager (DSM) ve verzi 6.1, který umožňuje instalaci nepřeberného množství aplikací, mimo jiné aplikace Surveillance Station, která slouží pro živé monitorování a záznamů bezpečnostních kamer. V ceně zařízení jsou dvě licence pro IP kamery zdarma, vzhledem k počtu IP kamer ve firmě EXTRAVÝFUK, s. r. o. a prodeji licencí po čtyřech kusech bude firma vlastnit licence až na čtrnáct IP kamer.

Pevný disk

Pro výběr pevných disků je nejdůležitější vědět potřebnou kapacitu pro uložení všech dat, která firma produkuje. Největší část z této kapacity připadne pro záznamy z bezpečnostních IP kamer. Při plánovaném počtu 11 kamer, rozlišení 1980 x 1080, 25 snímcích za sekundu, kompresním algoritmu H.264, trvalém záznamu a dobou archivace 14 dnů vychází kapacita na přibližně 2,7 TB. Dále bude potřeba kapacita 0,3 TB pro plné image čerstvě nainstalovaných a nastavených všech počítačů ve firmě,

a také přírůstkové image disků tak aby v případě jakýchkoliv softwarových a hardwarových problému bylo možné rychle obnovit zařízení do původního stavu. A nakonec kapacita 0,2 TB pro všechny ostatní citlivé firemní data. Celková potřebná kapacita bude tedy minimálně 3,2 TB. Souhrn potřebné kapacity lze vidět v Tabulce 4.8. Vzhledem k potřebné kapacitě včetně nějaké rezervy do budoucna bylo rozhodnuto o využití 3.5" HDD od firmy Western Digital, konkrétně 4 TB model z řady RED. Tyto disky budou muset být dva, jelikož z důvodu spolehlivosti a bezpečnosti dat budou disky spojeny do diskového pole. Tento typ disku je určený přímo pro provoz v síťových uložištích, kde bude využit 24 hodin denně, 7 dní v týdnu.

Účel	Potřebné místo
Citlivé firemní data	Celkem 0,2 TB
Záznam kamer	Celkem 2,7 TB
Image disku	Celkem 0,3 TB
- Notebook 1	70 GB
- Notebook 2	65 GB
- PC 1	55 GB
- PC 2	55 GB
- PC 3	55 GB
Celkem	**3,2 TB**

Tabulka 4.8 – Souhrn potřebné kapacity na disku

Zdroj: (vlastní)

Cenová kalkulace potřebných položek pro síťové zařízení lze nalézt v Tabulce 4.9.

Položka	Počet kusů	Cena za kus bez DPH	Cena celkem bez DPH
Synology DiskStation DS716+II	1	10 570,25 Kč	10 570,25 Kč
WD RED 4 TB	2	3 297,20 Kč	6 594,40 Kč
Synology 4 licence pro IP kamery	3	4 131,40 Kč	12 394,20 Kč
Celkem	**6**		**29 558,85 Kč**

Tabulka 4.9 - Položky síťového zařízení a jejich cenová kalkulace

Zdroj: TINT s. r. o., 2016 (vlastní zpracování)

4.4.3. Stolní počítač

Podle požadavků firmy na rozšíření o jeden stolní počítač, který bude umístěn ve skladu je navrhnuto řešení, a jeho specifikace včetně ceny jednotlivých položek bez DPH lze nalézt v Tabulce 4.10. Při návrhu tohoto stolního počítače bylo dbáno na kvalitu jednotlivých komponent (výrobce, záruční dobu,…) a přijatelnou cenu, tak, aby zařízení dokázalo bezproblémově a rychle fungovat v prašném prostředí ve skladu.

Položka	Počet kusů	Cena za kus bez DPH	Cena celkem bez DPH
ASROCK H110M-HDS	1	1 238,84 Kč	1 238,84 Kč
Intel Core i3-7100	1	2 719,01 Kč	2 719,01 Kč
NOCTUA NH-L9x65	1	983,47 Kč	983,47 Kč
Corsair 2GB DDR3 1333MHz CL9	2	387,60 Kč	775,20 Kč
Intel 540s 120GB	1	1 652,07 Kč	1 652,07 Kč
SilverStone ST30SF 300W SFX series	1	1 156,20 Kč	1 156,20 Kč
Fractal Design Node 804	1	2 461,16 Kč	2 461,16 Kč
Acer V226HQLBbd	1	2 189,26 Kč	2 189,26 Kč
ROLINE propojovací DVI-D, 2m	1	164,46 Kč	164,46 Kč
Hama AK-220	1	157,02 Kč	157,02 Kč
Logitech Corded Mouse M500	1	569,42 Kč	569,42 Kč
Microsoft Windows 10 Pro	1	5 205,79 Kč	5 205,79 Kč
Microsoft Office 2016 pro domácnosti a podnikatele	1	4 950,41 Kč	4 950,41 Kč
Celkem	**14**		**19 271,90 Kč**

Tabulka 4.10 - Specifikace stolního počítače a cenová kalkulace

Zdroj: TINT s. r. o., 2016 (vlastní zpracování)

4.5.Nastavení koncových zařízení v síti

V této podkapitole bude popsáno nastavení nových koncových zařízení v počítačové síti firmy, a to konkrétně síťových tiskáren, IP kamer a síťového uložiště.

4.5.1. Nastavení síťových tiskáren

Jako první bude nastavena u obou síťových tiskáren jejich IP adresa, kterou budou mít pevně přiřazenou. První tiskárna Epson L655 v kanceláři vedení bude mít přiřazenou IP adresu 192.168.1.36 s maskou sítě 255.255.255.0 a adresu výchozí brány bude nastavena na hodnotu 192.168.1.1. Druhá tiskárna Epson WorkForce M100 nacházející v kanceláři pracovníků bude mít nastavenou pevnou IP adresu 192.168.1.37 s maskou sítě 255.255.255.0 a taktéž adresu výchozí brány na hodnotu 192.168.1.1.

4.5.2. Nastavení IP kamer

U IP kamer budou taktéž nastaveny pevné IP adresy, pro jednotlivé kamery číslo 1 až 11 bude přidělen rozsah od 192.168.1.16 do 192.168.1.26 a adresa výchozí brány bude 192.168.1.1. Poté z důvodu bezpečnosti budou přenastaveny přihlašovací údaje, jako je přihlašovací jméno a heslo.

4.5.3. Nastavení síťového uložiště

Po instalaci dvou pevných disků do síťového uložiště a připojení zařízení k síti bude muset být nainstalován operační systém od firmy Synology, který se jmenuje DiskStation Manager (DSM). Toto se provede tak, že se do adresního řádku v internetovém prohlížeči zadá find.synology.com nebo diskstation:5000 a tímto se spustí nástroj Web Assistant, který začne vyhledávat síťové zařízení v místní síti. Jako první proběhne inicializace pevných disků a bude nastaveno vytvoření diskového pole RAID typu Synology Hybrid RAID (SHR), který je optimalizován pro zařízení Synology a při diskovém poli skládající se ze 2 disků jsou data odolné proti závadám na jednom disku. Dále se již pokračuje pomocí průvodce a ke konci bude výzva ke změně hesla k administrátorskému účtu, který se nazývá admin.

Změna síťového nastavení

Dále bude přenastaveno síťové nastavení. Bude nastavena pevná IP adresa 192.168.1.40 s maskou sítě 255.255.255.0 a výchozí bránou 192.168.1.1. Také bude přenastaveno jméno serveru, a to na DS716. Přístup na síťové zařízení bude buď přes webový prohlížeč a to přes adresu 192.168.1.40:5000, a nebo přes protokol SMB, pomocí kterého budou na koncových zařízeních se systémem Windows namapovány síťové disky. Adresa pro přístup k sdíleným složkám je \\DS716.

Vytvoření uživatelských účtů

Vytvoření uživatelských účtů je důležité z důvodu zavedení práv pro přístup k síťovému uložišti. Nastavená hesla budou mít z důvodu bezpečnosti minimálně 8 znaků kombinující malá a velká písmena, čísla a speciální znaky. Seznam vytvořených uživatelských účtů je vidět v Tabulce 4.11.

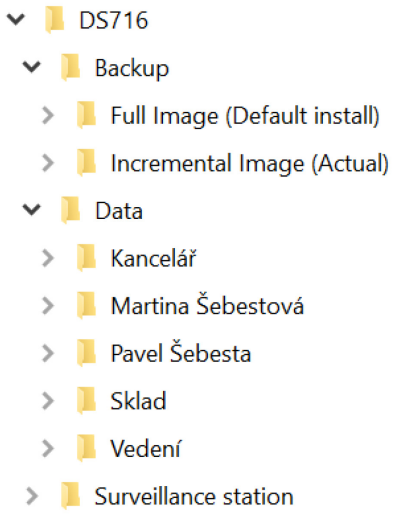
Uživatelské jméno	Heslo
admin	**********
SebestovaMartina	**********
SebestaPavel	*********
Kancelar	********
Sklad	********

Tabulka 4.11 - Seznam uživatelských účtů

Zdroj: vlastní

Vytvoření adresářové struktury

Defaultně vytvořené složky při instalaci budou smazány, a bude vytvořena hierarchie složek, aby byla všechna data přehledně uspořádaná. Bude vytvořena složka Backup pro plné image disků počítačů ve stavu čisté instalace operačního systému, programů a jejich nastavení a také pro přírůstkové image, které budou obsahovat aktuální stav počítačů. Dále bude vytvořena složka Data, která bude obsahovat veškerá citlivá firemní data a budou tříděna podle uživatelů. A nakonec složka Surveillance station, která bude obsahovat záznamy bezpečnostních kamer. Hierarchii sdílených složek lze vidět na Obrázku 4.3.



Obrázek 4.3 - Hierarchie sdílených složek

Zdroj: vlastní

Nastavení práv uživatelů

Z důvodu bezpečnosti dat na síťovém uložišti musí být nastavena hierarchie práv pro jednotlivé uživatele, která budou rozhodovat o tom, který uživatel bude mít kam přístup. Největší absolutní práva bude mít administrátorský účet admin, který se ale běžně nebude využívat. Přístupové práva pro ostatní uživatelské účty lze vidět v Tabulce 4.12, kde R jako read značí právo číst, W jako write právo zápisu a R/W jejich kombinaci.

Uživatelské jméno	Sdílená složka							Webové rozhraní DSM
		Data					Surveillance station	
	Backup	Martina Šebestová	Pavel Šebesta	Vedení	Kancelář	Sklad		
admin	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
SebestovaMartina	R/W	R/W	-	R/W	R/W	R/W	R	R/W
SebestaPavel	R/W	-	R/W	R/W	R/W	R/W	R	R/W
Kancelar	-	-	-	-	R/W	R	-	-
Sklad	-	-	-	-	R	R/W	-	-

Tabulka 4.12 - Práva uživatelských účtů

Zdroj: vlastní

Nastavení softwarového balíčku Surveillance Station

Operační systém DSM umožňuje instalaci softwarových balíčků, pro potřeby této bakalářské práce bude popsáno nastavení pouze balíčku Surveillance Station, který slouží pro správu IP kamer, živý náhled kamer tak pro vytváření záznamu z kamer a ukládání na síťové uložiště.

Vzhledem k využité značce a modelu IP kamer, které jsou v seznamu podporujících kamer, bude stačit vyhledat IP kameru podle IP adresy a přejmenovat jejich jméno. IP adresy jednotlivých kamer a jejich jméno lze nalézt v Příloze 1.

Dále budou nastaveny parametry pro záznam z bezpečnostních kamer. Bude se nahrávat v rozlišení 1920x1080 při 25 snímcích za sekundu, bude využit kodek H.264+ a doba záznamu nastavena na 14 dní. IP kamery i aplikace Surveillance Station umožnují využít různé nastavení pro dva streamy. Z důvodu malé propustnosti do sítě internet budou nastaveny parametry druhého streamu, který bude přístupný jako živý náhled z webového rozhraní systému DSM, tak, aby bylo umožněno plynulé zobrazování živého náhledu z kamer i z vnější sítě internet. Rozlišení živého vysílání bude 1280x720 při 15 snímcích za sekundu a bude využito kodeku H.264+.

4.5.4. Nastavení koncových zařízeních

Nakonec budou nastaveny všechny koncové zařízení jako Notebooky, stolní počítače a různé mobilní zařízení. Notebook a stolní počítače budou mít nastavenou pevnou IP

adresu podle Přílohy 1 s maskou sítě 255.255.255.0 a IP adresou výchozí brány 192.168.1.1. Dále budou nastaveny na těchto zařízeních zástupci síťových složek ze síťového uložiště, bude zadáno umístěni položky \\DS716 a následné zadání přihlašovacích údajů, které přísluší k danému účtu.

Všechny ostatní mobilní zařízení budou nastaveny na přijetí IP adresy automaticky z DHCP serveru.

5 Zhodnocení řešení počítačové sítě

V této kapitole bude navrhnuté řešení počítačové sítě a koncových zařízení zhodnoceno ze dvou hledisek. Konkrétně z hlediska finančního, funkčního a také zmíněná implementace řešení.

5.1. Finanční analýza návrhu

Navrhovanou změnu ve firmě můžeme rozdělit na dvě části. Tou první je samotná změna základních aktivních hardwarových prvků sítě. Finanční nákladnost tohoto kroku lze vidět v Tabulce 5.1, která ukazuje pouze ceny za zakoupení položek.

Položka	Celková cena bez DPH
Router	3 800,83 Kč
Switche	8 219,00 Kč
Access pointy	4 115,70 Kč
Celkem	**16 135,53 Kč**

Tabulka 5.1 - Kalkulace základních hardwarových prvků sítě

Zdroj: TINT, s. r. o., 2016 (Zpracování vlastní)

Další částí, kterou by bez té předchozí nebylo možné provést, je návrh koncových zařízení podle požadavků firmy. Finanční nákladnost tohoto kroku lze vidět v Tabulce 5.2, která také ukazuje pouze cenu za zakoupení položky.

Položka	Celková cena bez DPH
Síťové uložiště	29 558,85 Kč
IP kamery	31 727,30 Kč
Tiskárny	10 321,48 Kč
Stolní počítač	19 271,90 Kč
Celkem	**90 879,53 Kč**

Tabulka 5.2 - Kalkulace koncových zařízení

Zdroj: TINT, s. r. o., 2016 (Zpracování vlastní)

Celková cena za obě části je 107 015,06 Kč, i když v této ceně není započítána cena za UTP kabel, koncovky RJ-45, síťové zásuvky, krycí lišty a jiný drobný materiál, který se po domluvě s firmou TINT, s. r. o. bude platit až podle skutečně využitého počtu, firmou bylo rozhodnuto, že cena je adekvátní přínosu a nic nebrání realizaci implementace navrhnutého řešení.

5.2.Implementace navrhnutého řešení

Obchodní firma EXTRAVÝFUK, s. r. o. se rozhodla toto navrhované řešení implementovat a samotná realizace proběhla v prosinci 2016. Fyzickou instalaci hardwarových prvků realizovala firma ve své režii ve spolupráci s firmou TINT, s. r. o., na mně bylo pak již provést fyzické dokončovací práce (konektory na UTP kabelu, samotné zapojení kabelů do zařízení atd.) a nakonec nastavení všech zařízení v síti.

5.3.Funkční analýza návrhu

Implementované řešení, které vzniklo podle požadavků obchodní firmy již funguje pár měsíců, a lze říci, že navrhnuté a implementované řešení má pro firmu obrovský přínos. Kromě rozšíření počítačové sítě a zvýšení zabezpečení firmy včetně jejich dat, se ve firmě urychlily a usnadnily mnohé podnikové procesy, z čehož profitují jak zaměstnanci, tak vedení firmy.

Spolehlivost sítě se zvýšila natolik, že za celou dobu došlo jen k jedinému výpadku na straně ISP, kde důvodem k tomuto výpadku bylo to, že byl překopán v okolí jeden optický kabel, ale firma to téměř ani nepostřehla, jelikož redundantní připojení ve formě LTE připojení zafungovalo během minuty automaticky a jakmile byla závada vyřešena ze strany ISP, automatika zafungovala správně a s minimální časovou prodlevou přepnula zase zpět na VDSL připojení.

6 Závěr

Tato práce se zaměřovala na návrh počítačové sítě pro obchodní firmu EXTRAVÝFUK, s. r. o.

Než mohlo dojít k navrhnutí řešení počítačové sítě, bylo nejdříve nutné provést analýzu současné počítačové sítě a prostředí, ve kterém firma do té doby fungovala. Poté již podle zjištěných skutečností a podle požadavků firmy, bylo možné navrhnout vhodný síťový hardware, jejich následné fyzické a logické propojení a jejich nastavení. Poté byly vybrány vhodné koncové zařízení a následně popsáno jejich nastavení.

Obchodní firma se rozhodla navrhované řešení implementovat v prosinci 2016, a je pravděpodobné, že celá počítačová síť včetně koncových zařízení přinese firmě po mnoho následujících let více kladných vlastností, a to nejen zvýšenou spolehlivostí, dostupností a propustností připojení do sítě internet a vnitřní sítě LAN, ale také zvýšením zabezpečení majetku firmy včetně citlivých dat. Rozšíření počítačové sítě ušetři drahocenný čas vedení, ale také zaměstnancům, kde se mimo jiné zrychlí naskladňování a vyskladňování zboží. Díky těmto všem změnám došlo k rozšiřování a zjednodušování procesů ve firmě.

Všechny aktivní i pasivní síťové prvky a koncové zařízení jsou lehce naddimenzované tak, aby nebylo technické a morální zastarání tak rychlé. V případě dalšího rozšiřování sítě by bylo vhodné implementovat technologií VLAN a díky ní oddělit narůstající provoz sítě.

Na základě uvedených faktů byl cíl této bakalářské práce, který zahrnoval návrh počítačové sítě pro obchodní firmu splněn.

Seznam použité literatury

Odborná literatura

HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce.* 5. aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

KUROSE, James F. a Keith W. ROSS. *Počítačové sítě.* Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0538-5.

SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě*. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

TANENBAUM, Andrew S. and David J. Wetherall. Computer Networks 5th By Andrew S. Tanenbaum (International Economy Edition). Prentice Hall, Indian International Ed, 2010. ISBN 978-93-325-1874-2.

TRULOVE, James. *Sítě LAN: hardware, instalace a zapojení*. Praha: Grada, 2009. Profesionál. ISBN 978-80-247-2098-2.

Elektronické dokumenty a ostatní

3GPP – A Global Initiative: LTE-Advanced [online]. 2013 [cit. 2017-05-02]. Dostupné z: http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced

CETIN: Technologie VDSL3 v síti CETIN nabídne vyšší rychlosti internetového připojení [online]. [cit. 2017-05-02]. Dostupné z: https://www.cetin.cz/tiskove-centrum/-/asset_publisher/7E0pI2f3p5ci/content/technologie-vdsl3-v-siti-cetin -nabidne-vyssi-rychlosti-internetoveho-pripojeni?inheritRedirect=false&redirect=https%3A%2F%2Fwww.cetin.cz%2Ftiskove-centrum%3Fp_p_id%3D101_INSTANCE_7E0pI2f3p5ci%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_pos% 3D1%26p_p_col_count%3D2

Český telekomunikační úřad: Mapa pokrytí [online]. [cit. 2017-05-02]. Dostupné z: http://lte.ctu.cz/pokryti/

Hikvison Europe: DS-2CD2020F-I(W) [online]. [cit. 2017-05-02]. Dostupné z: http://www.hikvision.com/europe/Products_accessries_157_i8597.html

Khcn.Cinet [online]. [cit. 2017-05-02]. Dostupné z: http://khcn.cinet.vn/userfiles/file/2015/anh%20bai%20viet84/anh%200.jpg

Network World: IEEE sets new Ethernet standard that brings 5X the speed without disruptive cable changes [online]. 2016 [cit. 2017-05-02]. Dostupné z: http://www.networkworld.com/article/3124948/lan-wan/ieee-sets-new-ethernet-standard-that-brings-5x-the-speed-without-disruptive-cable-changes.html

Pinterest [online]. [cit. 2017-05-02]. Dostupné z: https://s-media-cache-ak0.pinimg.com/originals/99/a9/47/99a947d14809fc7797f8930bc906f9ae--cable-management-work-on.jpg

TINT, s. r. o.: Prodej výpočetní techniky [online]. 2016 [cit. 2017-05-02]. Dostupné z: http://www.tint.cz/it-reseni-a-sluzby/prodej-vypocetni-techniky/

Seznam zkratek

A. S.	Akciová společnost
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CAN	Campus Area Network
CSMA/CD	Carrier Senes Multiplne Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DIČ	Daňové identifikační číslo
DNS	Domain Name System
DPH	Daň z přidané hodnoty
DSL	Digital Subscriber Line
DSM	DiskStation Manager
EDGE	Enhanced Data rates for GSM Evolution
FTP	File Transfer Protocol
Gb/s	Rychlost v Gbitech za sekundu
GHz	Gigahertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HDD	Hard Disk Drive
HSDPA	High-Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IČO	Identifikační číslo osoby
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

ISO/OSI	International Organization for Standardization / Open Systems Interconnection
ISP	Internet service provider
LAN	Local Area Network
LTE	Long Term Evolution
MAN	Metropolitan Area Network
Mb/s	Rychlost v Mbitech za sekundu
MHz	Megahertz
NAS	Network Attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input Output System
PAN	Personal Area Network
PAT	Port Address Translation
POE	Power Over Ethernet
POP3	Post Office protocol
PSK	Pre-Shared Key
QOS	Quality of Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
S. R. O	Společnost s ručením omezeným
ScTP	Screened Twisted Pair
SHR	Synology Hybrid RAID
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSID	Service Set Identifier

SSL	Secure Sockets Layer
STP	Shielded Twisted Pair
TCP	Transmition Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporary Key Integrity Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDSL	Very high bit rate digital subscriber line
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WI-FI	Wireless-Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Acces

Prohlašuji, že

- jsem byl seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 4. 5. 2017

.....

Jakub Kyselý

Seznam příloh

Příloha 1

Jméno zařízení	Typ zařízení	IP adresa	MAC adresa
VDSL Router	ASUS DSL-AC68U	192.168.1.1	74:D0:2B:64:F0:B0
Switch 1	TP-Link TL-SG108PE	192.168.1.2	1A:EF:47:48:DB:3B
Switch 2	TP-Link TL-SG108PE	192.168.1.3	13:BE:8E:44:16:C1
Switch 3	TP-Link TL-SG108PE	192.168.1.4	77:48:2F:71:B7:12
Switch 4	TP-Link TL-SG108PE	192.168.1.5	B3:3E:6A:95:5A:8D
Switch 5	TP-Link TL-SG108PE	192.168.1.6	5D:90:74:CE:C4:E8
Rezerva pro Switch	-	192.168.1.7	-
Rezerva pro Switch	-	192.168.1.8	-
Rezerva pro Switch	-	192.168.1.9	-
Rezerva pro Switch	-	192.168.1.10	-
Access Point 1	Asus RP-AC66	192.168.1.11	E1:02:F2:3A:5F:9C
Access Point 2	Asus RP-AC66	192.168.1.12	0F:69:79:FB:52:82
Rezerva pro Access Point	-	192.168.1.13	-
Rezerva pro Access Point	-	192.168.1.14	-
Rezerva pro Access Point	-	192.168.1.15	-
IP CAM 1	Hikvision DS-2CD2020F-I	192.168.1.16	5B:6A:06:21:E4:75
IP CAM 2	Hikvision DS-2CD2020F-I	192.168.1.17	A6:11:4A:DD:F1:3A
IP CAM 3	Hikvision DS-2CD2020F-I	192.168.1.18	45:63:A9:74:03:8C
IP CAM 4	Hikvision DS-2CD2020F-I	192.168.1.19	92:FD:F8:05:88:2B
IP CAM 5	Hikvision DS-2CD2020F-I	192.168.1.20	8D:D4:AA:42:A9:00
IP CAM 6	Hikvision DS-2CD2020F-I	192.168.1.21	B6:A8:A4:6F:37:FF
IP CAM 7	Hikvision DS-2CD2020F-I	192.168.1.22	41:8A:CF:4C:31:05
IP CAM 8	Hikvision DS-2CD2020F-I	192.168.1.23	02:B7:F5:F9:2F:44
IP CAM 9	Hikvision DS-2CD2020F-I	192.168.1.24	81:96:0B:EE:83:19
IP CAM 10	Hikvision DS-2CD2020F-I	192.168.1.25	CA:55:23:3C:F7:A6
IP CAM 11	Hikvision DS-2CD2020F-I	192.168.1.26	41:EF:BB:F2:E3:2B
Rezerva pro IP Kameru	-	192.168.1.27	-
Rezerva pro IP Kameru	-	192.168.1.28	-
Rezerva pro IP Kameru	-	192.168.1.29	-
Rezerva pro IP Kameru	-	192.168.1.30	-

Rezerva pro IP Kameru	-	192.168.1.31	-
Rezerva pro IP Kameru	-	192.168.1.32	-
Rezerva pro IP Kameru	-	192.168.1.33	-
Rezerva pro IP Kameru	-	192.168.1.34	-
Rezerva pro IP Kameru	-	192.168.1.35	-
Printer 1	Epson L655	192.168.1.36	60:19:07:21:01:52
Printer 2	Epson WorkForce M100	192.168.1.37	7A:D7:09:18:83:87
Rezerva pro tiskárnu	-	192.168.1.38	-
Rezerva pro tiskárnu	-	192.168.1.39	-
NAS	Synology DiskStation DS716+II	192.168.1.40	F6-07-13-96-F7-5E
Rezerva pro síťové uložiště	-	192.168.1.41	-
Notebook 1	Surface Pro 4	192.168.1.42	39:83:E4:89:A4:DB
Notebook 2	Surface Pro 4	192.168.1.43	80:F3:93:BB:D3:DB
PC 1	Poskládaný stolní počítač	192.168.1.44	38:F8:67:E2:94:31
PC 2	Poskládaný stolní počítač	192.168.1.45	AA:B4:D6:70:BE:5F
PC 3	Poskládaný stolní počítač	192.168.1.46	7E:5A:79:E9:1C:BB
Rezerva pro koncové zařízení	-	192.168.1.47	-
Rezerva pro koncové zařízení	-	192.168.1.48	-
Rezerva pro koncové zařízení	-	192.168.1.49	-
Rezerva pro koncové zařízení	-	192.168.1.50	-

Příloha 1 - Seznam zařízení a jejich IP a MAC adresy

Zdroj: vlastní